Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Experimentální síť 4G na platformě openLTE

4G Experimental Network on openLTE platform

2016 **Bc. Martin Kulíšek**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Martin Kulíšek**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Experimentální síť 4G na platformě openLTE
4G Experimental Network on openLTE Platform

Jazyk vypracování: čeština

Zásady pro vypracování:

1. Vývoj mobilních sítí, koncept LTE a IMS.
2. USRP a open-source projekt GNU Radio.
3. Návrh a praktická realizace prvku eNodeB pomocí openLTE.
4. Dosažené výsledky a zhodnocení použití openLTE.

Seznam doporučené odborné literatury:

[1] N. Nikaein, R. Knopp, F. Kaltenberger, L. Gauthier, Ch. Bonnet, D. Nussbaum and Riadh Ghaddab, OpenAirInterface 4G: an open LTE network in a PC. Eurecom, FRance, 2014.
[2] M. Prokeš, Bezpečnostní problémy GSM. VŠB-TU Ostrava, diplomová práce, 2014. URL http://hdl.handle.net/10084/103798.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **doc. Ing. Miroslav Vozňák, Ph.D.**

Datum zadání: 01.09.2015
Datum odevzdání: 29.04.2016

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *26. dubna 2016*

Zulčík
.....
podpis studenta

Poděkování

Úvodem bych chtěl poděkovat vedoucímu práce doc. Ing. Miroslavu Vozňákovi, Ph.D. za vedení, odbornou pomoc a konzultace při vytváření této diplomové práce.

Abstrakt

Diplomová práce popisuje vytvoření přístupového bodu eNodeB, vlastní LTE sítě s využitím otevřeného zdrojového kódu openLTE a softwarově definovaného rádia USRP B210. Teoretická část je zaměřena na historii mobilních technologií, na technologii USRP a projektu GNU Radio. Praktická část práce je věnována samotné problematice vytvoření přístupového bodu. Jsou zde popisovány jednotlivé kroky, konfigurace jednotlivých prvků, aktuální verze systému a problémy, které vznikly při realizaci. Závěr práce je zaměřen na celkové shrnutí, zhodnocení úspěšnosti realizace projektu openLTE s možností reálného použití v praxi.

Klíčová slova

openLTE, USRP B210, eNodeB, UE, mobilní zařízení, mobilní síť.

Abstract

Thesis describes creating accession point eNodeB, own LTE network with utilizing open-source code openLTE and define software radio USRP B210. Teoretical part is focused on history of the mobile technology, on technology USRP and project GNU Radio. Practical part of the work is devoted to very own problematic fracture of accession point. There are defined single steps, configuration of the individual features, actual version of the system and problems which were created with realisation. Conclusion is focused on general summary, judging success of project realisation openLTE and options in real usage in practice.

Key words

openLTE, USRP B210, eNodeB, UE, mobile device, mobile network.

Seznam použitých zkratek

Zkratka	Význam	Český překlad
PPT	Push-to-Talk	
MTS	Mobile Telephone Service	
OLT	Norwegian for Offentlig Landmobil Telefoni	
MTA(B,C,D)	Mobiltelefonisystem A(B,C,D)	
ARP	Autoradiopuhelin	
AMR	Automated City Radiophone	
AMPS	Advanced Mobile Phone Systém	
TAC	Total Access Communication Systém	
GMSK	Gaussian Minimum Shift Keying	
NMT	Nordisk Mobile Telephony	
FFSK	Fast Frequency Shift Keying	
GSM	Groupe Spécial Mobile	
GPRS	General Packet Radio Service	
EDGE	Enhanced Data rates for GSM Evolution	
CSD	Circuit Switched Data	
HSCSD	High Speed Circuit Switched Data	
CDMA	Code Division Multiple Access	
CDPD	Cellular Digital Packet Data	
iDEN	Integrated Digital Enhanced Network	
PDC	Personal Digital Cellurar	
PHS	Personal Handy-phone Systém	
UMTS	Universal Mobile Technology System	

3GPP	3rd Generation Partnership Project	
ETSI	European Telecommunications Standards Institute	
ITU	International Telecommunication Union	
FDD	Frequency Division Duplex	
TDD	Time Division Multiplex	
FDMA	Frequency Division Multiple Access	
TDMA	Time Division Multiple Access	
HARQ	Hybrid Automatic Repeat Request	
HSS	Home Subscriber Server	Uchovávání informací o uživatelích
Ki		Účastnický ověřovací klíč
Kc		Šifrovací klíč
open-source		otevřený zdrojový kód
UHF	Ultra High Frequency	Ultra krátké vlny
VHF	Very High Frequency	Velmi krátké vlny
PROM	Programmable Read Only Memory	Programovatelná paměť
ISDN	Integrated Services Digital Network	Digitální síť integrovaných služeb
IMS	IP-Multimedia Subsystem	IP multimediální subsystém
SS7	Signaling System Number 7	Signalizační systém č.7
MIMO	Multiple-Input Multiple-Output	Více vstupů více výstupů
QoS	Quality of Service	Kvalita služeb
LTE	Long Term Evolution	Technologie pro vysokorychlostní přenos dat v mobilních sítích
LTE+	Long Term Evolution Advanced	Rozšířená technologie pro vysokorychlostní přenos dat v mobilních sítích
openLTE	Open Long Term Evolution	Otevřený kód pro technologii pro vysokorychlostní přenos dat v mobilních sítích

USRP	Universal Software Radio Peripheral	Softwarově definované rádio
uSIM	Universal Subscriber Identity Module	Univerzální účastnická identifikační karta
UHD	USRP Hardware Driver	Ovladač pro USRP
IMSI	International Mobile Subscriber Identity	Identifikátor SIM karty
IMEI	International Mobile Equipment Identity	Identifikátor mobilního telefonu
UE	User Equipment	Koncové zařízení
eNodeB	Evolved NodeB	Základová stanice pro LTE
VoLTE	Voice over LTE	Možnost přenášet hlas přes LTE
SDR	Software Defined Radio	Softwarové rádio
IP	Internet Protocol	Internetový protokol
IPsec	Internet protocol Security	Zabezpečení protokolu IP
FPGA	A field-programmable Gate Array	Programovatelné hradlové pole

Obsah

Úvod

Pokrok v mobilních technologiích nám výrazně zjednodušil život. Dnes už se nejedná pouze o hovory nebo SMS služby, ale hlavně jde multimediální služby a přístupu na internet. Vzhledem k tomu, že uživatelé mobilních technologií mají požadavky na rychlejší mobilní připojení, tak operátoři a ostatní vývojoví pracovníci se snaží v této oblasti využívat nových trendů a inovovat stávající systémy. Jednou z cest, jak vytvořit nové konkurenční prostředí v této oblasti je inovace a rozvoj technologie LTE. V současnosti se stala tato technologie velmi populární a je málo míst na zemi, kde by nebyla zavedena. V dnešní době se na internetu objevují simulace nebo emulace, kde si uživatel může vyzkoušet, testovat a lépe porozumět mobilní síti LTE. Jeden takový projekt, který je volně ke stažení má označení openLTE.

V této práci bude popsán postup, jak jsi vytvořit takový přístupový bod pomocí projektu openLTE a desky USRP B210. Dále budu uvádět veškeré postupy a problémy, které nastanou při vytváření takového přístupového bodu. Celou práci budu psát s vědomím, že čtenář zná základní terminologii v mobilních sítích a příkazech v operačním systému Linux.

V kapitole jedna a dvě, bude popsán stručný přehled mobilních sítí od 0G po 4G. A detailní popis konceptu ISM a LTE. V kapitole dvě bude popsána rádiová periferie USRP a projekt GNU Radio.

V kapitole tři popíši postup, jak si vybudovat vlastní přístupový bod eNodeB a zároveň jaké problémy se vyskytly při realizaci.

Poslední část této diplomové práce bude obsahovat celkové zhodnocení projektu openLTE a dosažených výsledků.

1 Vývoj mobilních technologií, koncept LTE a IMS

1.1 Sítě nulté generace (0 - 0,5G)

Vývoj prvních mobilních sítí vznikal v průběhu druhé světové války, kdy komunikace probíhala pomocí vybudovaných radiostanic mezi tanky. V sovětském svazu komunikoval velitel tanku s ostatními tanky a ty směli jen poslouchat rozkazy velitele, naopak americké tanky mohli komunikovat obousměrně. Po skončení druhé světové války se tento způsob komunikace rozšířil a začaly se vyvíjet potřebné technologie. V této generaci neexistoval buňkový systém a komunikovalo se na základě vybudovaných základových stanic, které umožňovali komunikaci s koncovými zařízeními. O každé spojení se staral operátor. První takovou technologií byla PPT (Push to Talk), kde po stlačení tlačítka se zahájila komunikace, a po uvolnění tlačítka se kanál ukončil, aby mohl vyslechnout druhou stranu. I dnes tuto technologii vidíme převážně mezi policisty, hasiči a záchranáři. Teď se podíváme na nejdůležitější technologie, které patří do této generace [3].

1.1.1 MTS

MTS vznikla v Bellových laboratořích a poprvé byla spuštěna v St. Louis v roce 1946. Zařízení mělo váhu 36 kg, které umožňovalo v metropolitních oblastech pouze 3 kanály pro všechny uživatele, a později se přidaly další kanály a celkem mohla mít až 32 kanálů pro celé 3 pásma. Tato technologie přetrvala do roku 1980 převážně v Severní Americe. V některých místech proběhla výměna později. Používala 25 VHF rádiových kanálů ve Spojených Státech a Kanadě. Kvůli hmotnosti zařízení ji uživatel nemohl mít stále u sebe, ale bylo nutné ji instalovat do motorového vozidla a samotná komunikace probíhala half-duplexem. Tyto kanály byly náchylné k přetížení a rušení sítě. MTS je vylepšená technologie PTT, kde po sepnutí tlačítka se uživatel propojil se základovou stanicí a spojovatel přepojil spojení k cíli. Později byla nahrazena lepší telefonní službou IMTS (Improved Mobile Telephone Service), která vznikla v roce 1964. Zlepšení nastalo hlavně v přímém připojení účastníků než spojení přes operátora. Dalším nástupcem v technologii MTS bylo AMTS (Advanced Mobile Telephone System) [3].

1.1.2 OLT

I u nás v Evropě byly návrhy na mobilní sítě. První taková mobilní sít byla v Norsku. Měla označení OLT a vznikla v roce 1966. Jednalo se o první ruční mobilní telefon a samotná síť pracovala na VHF 160 MHz, kde mobilní jednotka pracovala na frekvenčním rozmezí od 160-162 MHz a základová stanice 168-170 MHz. Jako u technologie MTS se jednalo o half-duplex přenos (dražší verze mobilního zařízení umožňovala duplex přenos). O pár let později byla rozšířena o UHF pásmo a v roce 1976 dokonce umožňovala mezinárodní roaming ve skandinávských zemích [3].

1.1.3 **MTA**

Ještě dříve než OLT byla vyvinuta ve Švédsku technologie MTA. Byla představena v roce 1956 a fungovala do roku 1967. Jednalo se o první automatický mobilní telefon, který umožňoval přímé volání účastníků bez pomoci operátora. Dostupná byla pouze ve Stockholmu a Gothenburgu. Pracovala na frekvenci 160 MHz a celkový počet předplatitelů bylo sto dvacet pět a většinou ji využívali banky. Následně byla tato technologie vylepšena a měla označení MTB, která byla představena v roce 1962 a fungovala do roku 1983. Pracovala na frekvenčním rozsahu od 77,5 MHz a 81-82,5 MHz. Poslední verzí této technologie byla MTD. Byla představena v roce 1971 a fungovala do roku 1987. V podstatě to byl ruční mobilní telefon, který pracoval na frekvenčním pásmu 450 MHz. Technologie MTD měla přes dvacet tisíc účastníků a tento typ sítě byl vybudován v Dánsku a Norsku. Systém MTA byl demontován v roce 1969 [1] [3].

1.1.4 **ARP**

V roce 1968 ve Finsku vznikl nápad na první auto-rádio telefon. Tato technologie měla označení ARP a stavba této sítě započala v roce 1971. Dokázala 100%tního geografického pokrytí za použití 140 základových stanic. Řadíme ji to 0,5G a měla velký úspěch, protože ještě před vznikem měla tato síť přes 10 tisíc uživatelů a o devět let později bylo zaznamenáno přes 35 tisíc uživatelů. Provozovala se na osmi kanálech s frekvencí 150 MHz, její vysílací výkon se pohyboval od 1 - 5 W a přenos byl half-duplex. Velikost jedné buňky měla okolo 30 km. Nevýhodou bylo, že mobilní terminály byly příliš velké a drahé, takže jsi je nemohl dovolit každý. Kvůli těmto problémům se Autotel rozhodl vytvořit konkurenta PALM (Publick Automated Land Mobile) [5] [11] [16].

1.1.5 **B-Netz**

I Západní Německo přišlo s vlastním nápadem na mobilní sít v roce 1972 a bylo vybudováno B-Netz. Síť fungovala do roku 1994 a tento systém byl realizován i v Dánsku, Nizozemsku a Lucembursku. Měl k dispozici 38 kanálů (u vylepšené B2-Netz až 78 kanálů). Počet základových stanic, které byly vybudovány, bylo 158 a v roce 1986 pracovaly pro 27 tisíc uživatelů. Později byla tato technologie nahrazena C-Netz a spuštěna v roce 1985 [2].

1.1.6 **AMR**

Ani vývoj v ČSSR nezahálel a v roce 1978 byla vyvinuta mobilní sít s označením AMR někdy taky označení jako AMRAD. Jednalo se experimentální sít, kterou vyvinula Tesla a pracovala na frekvenčním rozsahu 162-176 MHz. O pět let později byl spuštěn celorepublikový provoz na frekvenčním rozmezí od 161-167 MHz a za další čtyři roky se zprovoznili i oblastní sítě na frekvenčním rozmezí 152-157 MHz. Nevýhodou bylo to, že ne každý mohl tuto síť používat, ale jen vybraní uživatelé.

Naopak výhoda této technologie byla, že se dokázala vyrovnat západní technologii a byla i celkem pokroková. Fungovala po celých 14 let a v roce 1999 byla sít vypnuta [4].

1.2 Sítě první generace (1G)

V této generaci došlo ke zlepšení parametrů z předcházející generace a byla vylepšena o nový buňkový systém, který byl základním kamenem pro následující generace. Jedná se analogově telekomunikační standardy, které byly zavedeny v roce 1980 a postupně nahrazovaly 2G technologie, které budou již digitální.

1.2.1 AMPS

Pro AMPS byl vyvinut mobilní telefon vyrobený v Bellových laboratořích a byl představen v roce 1983 v Americe a používal se do roku 2000. V této technologii byla poprvé využita myšlenka buňkového systému, na kterém se podílela i Motorola. Motorola měla na starost sestrojit mobilní zařízení a Bellovy laboratoře vyvinuly mobilní síť tak, aby telefon na tuto síť fungoval. První mobilní telefon, který fungoval na systému AMPS měl označení DynaTAC 8000x. Každý telefon byl vybaven třiceti dvou bitovým sériovým číslem a desítimístným telefonním číslem uloženým v paměti PROM. AMPS je první generací mobilních technologie která začala používat oddělené frekvence (kanály) u každého hovoru (FDMA) s 30 kHz odstupem kanálů a 70 MHz šířkou pásma (824 – 894 MHz). Kámen úrazu byl fakt, že z hlediska bezpečnosti byla tato technologie absolutně bezbranná. Samotná ochrana odposlouchávání nebyla žádná a to díky analogovému přenosu, takže účastníkovy stačil "skener", pomocí kterého mohl slyšet telefonní hovory. Tento systém se využíval hlavně v Severní Americe, později i Austrálie a Izrael. V Americe se tato technologie celkem dlouho udržela. Později AMPS byla zdigitalizována a dostala označení D-AMPS (Digital AMPS), často označované jako TDMA. D-AMPS byla nasazena v roce 1993 a už je řazena spíše do 2G [6] [7].

1.2.2 TACS

Zastaralejší varianty AMPS byli TACS a ETACS. Tyto mobilní systémy využívaly v zemích Spojeného království od roku 1983 a později byly použity i v Evropě. I Japonsko tuto technologii vlastnilo, ale pod názvem JTAC (Japanese Total Access Communication) a dalším místem využití bylo v Hong Kongu Číně. ETACS byla rozšířenější verze TACS s více kanály [6] [7].

1.2.3 C-Netz

C-Netz byla nová verze technologie A-Netz, B-Netz a B2-Netz, která byla hojně užívána v Západním Německu a využilo standardu C450. C-Netz byla poslední verze z analogových mobilních telefonů. Další verze byli D-Netz (GSM-900) a E-Netz (GSM-1800),

které byli již digitalizované. C-Netz byla představena v roce 1985 a vzhledem k problémům které měl B-Netz bylo přijetí C-Netztu velmi vysoké, kvůli většímu pokrytí. Celkem měla tato technologie kolem 800 tisíc uživatelů do roku 1990. Velikost primárních buněk byl mezi 15-20 km a mikro-buněk 2-3 km. Šířka pásma byla 20 kHz a byl určen pro 450 MHz. Technologie C-Netz byla ukončena roku 2000. Standardní C450 byla vyvinuta společností Siemens v roce 1980 [7] [8].

1.2.4 **Mobitex**

Švédská společnost Ericsson vyvinula roku 1988 novou technologii s názvem Mobitex. Tato technologie umožňovala přepojování paketů v datové síti. Mobitex klad důraz na bezpečnost a spolehlivost. Do provozu byla uvedena v roce 1986. Šířka kanálu byla 12,5 kHz. V Severní Americe používali frekvence 900 MHz a v Evropě běželi na 400-450 MHz. Mobitex využívala modulace GMSK. Mobitex byl nabízen do 30 sítí na 5 kontinentech. Do roku 2005 zůstal pouze v Americe a Kanadě zatímco celou Evropu ovládla nová technologie s názvem GSM. Podle informací Mobitex fungoval ještě déle v zemích Nizozemsko, Belgie a Lucembursko. Švédsko ukončilo Mobitex v roce 2012, systém pracoval 25 let [8] [9].

1.2.5 **DataTAC**

Další technologie, která byla vyvinuta v této generaci, měla označení DataTAC. Vyvinula ji společnost Motorola a byla nasazena ve Spojených Státech a samotná datová síť měla název Ardis. DataTAC vznikla v polovině roku 1990. Velmi podobná technologie s názvem MDI DataTAC byla používána v Hong Kongu jako Hutchison. DataTAC je otevřený standard typu bod-bod datové komunikace, velice podobný technologii Mobitex. V Severní Americe pracovala technologie v pásmu 800 MHz a byla nasazena i v Austrálii. Síť fungovala s přenosovou rychlostí 19,2 kbit/s, měla 25 kHz kanály ve frekvenčním pásmu 800 MHz.

1.2.6 **NMT**

Poslední technologie, která patří do 1G a je celkem podstatná má označení NMT. Byla spuštěna roku 1981 v zemích Dánsko, Finko, Norsko, Švédsko a Saudská Arábie a později se přidali další země. Tato technologie pomohla ostatním s přetížením a těžkými požadavky na mobilní telefony. NMT měla dvě varianty, první se označovala NMT-450 a druhá NMT-900. Čísla označují frekvenční pásmo, na kterém pracují. NMT-900 nese více kanálů a byla vydána v roce 1986. NMT-450 byla věnována švédskému Nordisk Mobiltelefon (později Ice.net a potom na Net 1, která postavila CDMA 450). Velikost buněk byl od 2 do 30 km a využívá plně duplexní přenos. Hlasový kanál je přenášen s FM modulací, pomocí FFSK. I zde byla nevýhoda bezpečnost, protože hlasová komunikace nebyla šifrována. Proto ji bylo možné lehce odposlouchávat. Pro zavedení datového přenosu dat NMT zaveden jednoduchý režim, který se označoval DMS (Data a Messaging Service) nebo NMT-Text. NMT se vyznačovala svobodností a otevřeností, což umožňovalo vyrábění hardwaru podle sebe. Byl velmi důležitý

pro společnosti Nokia a Ericsson. NMT ovládlo severské, pobaltské země a udržela se na scéně poměrně dlouho. Po zavedení GMS a přechod na digitální sítě NMT postupně ztrácelo klientelu a oficiálně byly NMT technologie ukončeny v roce 2010 [6] [7] [10].

1.3 Sítě druhé generace (2G)

Druhá generace mobilních sítí je přelomová z důvodu přechodu z analogového přenosu na digitální přenos. Dále pak lepší využití pásma, možnosti šifrování digitálního signálu, lepší služby, zajištění kvality hovorů, datové přenosy a další služby, bez kterých si svět nedokážeme už představit. Buňkový systém, který byl vyvinut v první generaci se zachoval, stejně tak i digitální signalizace pro přepojení rádiových stanic do zbytku telefonního systému. Nyní se podíváme na technologie druhé generace.

1.3.1 GSM

Vůbec nejznámější technologií je GSM, která byla vyvinuta ETSI a popisuje protokoly druhé generace. Digitální buňkový systém byl poprvé používán ve Finsku a od roku 1991 se stal základním kamenem pro celý svět a jako první systém bude pracovat na TDMA. Od roku 2014 se GSM stala celosvětovým standardem pro mobilní komunikaci, která má více než 90% podíl na trhu a působí ve více než 219 zemích a územích. CEPT (European Conference of Postal and Telecommunications Administrations) se v roce 1982 rozhodl vytvořit standard pro digitální mobilní hlasovou telefonii a cílem bylo vyvinout a nasadit společný mobilní telefonní systém v celé Evropě. Tyto pravidla byla předána EU, aby se GSM stalo povinnou normou. Nakonec se stala tato síť větší než ve Spojených Státech. Evropská komise v roce 1986 vyhradila pásmo pro GSM 900 MHz a první hovor přes tuto síť uskutečnil bývalý finský premiér Harri Holkeri do Kaarina Suonio v roce 1991 a v roce 1992 byla odeslaná první SMS (Short Message Service) ze Spojeného království do Finska. GSM po spuštění získalo velkou oblibu a bylo nutné rozšířit normu. Proto se v roce 1991 započalo s rozšířením z 900 MHz na 1800 MHz. První GSM-1800 byla nasazena ve Spojeném království v roce 1993 a i Austrálie v tomto roce spustila první GSM a byla úplně první mobilní sítí, která byla mimo Evropu. O dva roky později byla přidána služba faxu a datového provozu. Ve Spojených státech se nasadila GSM, která pracovala na frekvenci 1900 MHz. Celkový počet uživatelů překročil 10 miliónů a v roce 2004 nakonec bylo přes jednu miliardu uživatelů přihlášených v GSM síti. Následně přišli další nadstavby GSM první z ní byla GPRS a později EDGE. Zabezpečení v GSM nebylo nijak kvalitní. První bezpečnostní problém, který publikoval Ianem Golberg a Marcem Bricenem, bylo klonování SIM karty, kdy bylo možné získat IMSI a Ki klíč a na základně těchto hodnot se mohla naklonovat nová SIM karta a dala se použít pro extra placené hovory a zneužívání identity. Z pohledu operátora se dala využít falešná GSM, která získávala informace od MS. Posledním známým útokem je prolomení algoritmu A5. Tuto vážnou chybu odhalil Ian Goldberg, který mohl prolomit algoritmus z obyčejného PC a s kombinací s falešnou GSM stanicí mohl získat Kc klíč pro komunikaci šifrovanou libovolným algoritmem.

Dalším problémem je zabezpečení vnitřní síťe GSM, kdy lze získat přístup k částem HLR, VLR nebo AuC. V současné době se již systém GSM chystá vypnutí v USA přibližně v roce 2017. Hlavním důvodem je, že v GSM už nevidí budoucnost a chtějí tak dát příležitost moderním mobilním sítím. Stejně tak v Singapuru společnost M1, Singtel a StarHub chce ukončit GSM ve stejném roce, jako americká společnost AT&T. Austrálie vypíná GSM v roce 2016. Evropa plánuje ukončení v roce 2025. Čeští operátoři chtějí vypínat GSM přibližně v roce 2020, podle toho kdy jim vyprší licence, pro frekvenční pásma [14] [15] [18] [30].

1.3.2 **CSD**

CSD je nová forma přenosu pro TDMA a systémy založené na GSM. Velmi rychle klesla obliba a byla nahrazena GPRS a EDGE (E-GPRS). Přenos dat se prováděl pomocí modemu, který byl buď vestavěný do telefonu, nebo byl k němu připojený. Tyto systémy byly omezeny kvalitou zvukového signálu na 2,4 kbit/s nebo ještě méně. Volání funguje stejně jako v normálním hlasovém hovoru GSM, kdy jeden vyhrazený rádiový slot je rozdělen mezi telefonem a základovou stanicí [17].

1.3.3 **D-AMPS**

D-AMPS je rozšířením původního AMPS, které se zmodernizovalo z analogového přenosu na digitální. Někdy se označovalo IS-54 nebo IS-136. Toto rozšíření se projevilo spíše ve Spojených Státech a Kanadě, kde byla nasazena v roce 1993. Bohužel většinu stávající sítě byla nahrazena technologií GSM, GPRS a CDMA2000. Tento systém se nejčastěji označuje TDMA. D-AMPS využívá existujících kanálů a umožňuje plynulý přechod mezi digitálním a analogovým systémem v téže oblasti. Šifrování digitálních signálů využíval algoritmu (RCHP). K ukončení došlo v roce 2009 a přešlo se na nový systém s označením CDMA2000 [19].

1.3.4 **iDEN**

iDEN se nazývala sociální sítí a vyvinula ji společností Motorola. Původně iDEN měla mít označení MIRS (Motorola Integrated Radio System), začala v roce 1991 a přejmenována byla v roce 1994. Mobilní síť iDEN dokázala podporovat buď tři, nebo šest uživatelů. Fungovala na principu PTT za pomoci TDMA čímž se eliminoval duplexní přenos. I dnes ještě tato technologie funguje a neustále se využívá v zemích Kanada, Argentina, Mexiko, Singapur, Saudská Arábie. Jen Spojené Státy Americké ji v roce 2013 ukončili [20].

1.3.5 **PDC**

Předplatitelů pro tuto technologii byla spousta, ale pouze dočasně, protože byla vyřazena 3G technologiemi (W-CDMA a CDMA2000). Z celkového počtu 80 miliónů předplatitelů se na konci března počet snížil na 200 000. Stejně jako GSM, D-AMPS taky používá TDMA. PDC se standardizoval v roce 1991 a oficiálně zahájil službu v roce 1993, kdy používal 25 kHz nosnou a $\pi/4$ DQPSK.

Modulaci s třemi timesloty rychlostí přenosu 11,2 kbit/s a nebo šest timeslotů s rychlostí 5,6 kbit/s. PDC 800MHz měl implementovaný sestupný směr 810-888 MHz a vzestupný směr 893-958 MHz. A 1,5GHz měl sestupný směr 1477-1501 MHz a vzestupný směr 1429-1453 MHz. Výrobci síťových zařízení byl Ericsson a NEC. Datové služby fungovaly do 9,6 kbit/s (CSD) s přepojováním paketů bezdrátového datového přenosu s rychlostí 28,8 kbit/s (PDC-P) a hlasové kodeky byly PDC-EFR a PDC-HR. Problémy měla s udržením spojením, hlavně v uzavřených prostorách (např. výtahy) [21].

1.3.6 **PHS**

PHS byla vyvinuta v Japonsku v roce 1989 a měla mnohem jednodušší implementaci a nasazení než PDC a GSM. Měla přezdívku buněčný "chudák". Pracuje v pásmu 1880 - 1930 MHz, který se používá především v Japonsku a Číně. PHS je v podstatě bezdrátový telefon (podobný DECT), který má schopnost předávání dat z jedné buňky do druhé. Buňky jsou podstatně menší než u GSM a CDMA a to nejvýše do sto metrů. PHS se hodí do hustě osídlených městských oblastí, ale je velmi nepraktická do venkovních oblastí a rychle jedoucích vozidel. Používá hlasového kodeku ADPCM a metodu přístupu TDMA/TDD. Rozšířená verze PHS podporuje i vysokorychlostní datový přenos s rychlostí až 64 kbit/s nebo vyšší. Základnové stanice jsou kompatibilní s ISDN. V Číně měla být ukončena v roce 2011 [22] [23].

1.4 **Sítě přechodové druhé generace (2,5G - 2,75G)**

Do přechodových generací patří následující technologie. Jejich hlavní úlohou je zlepšení parametrů pro datové přenosy přes mobilní síť. Všechny uvedené technologie se používaly, nebo používají pro GSM a jejich druhou úlohou je lepší migrace do 3G.

1.4.1 **HSCSD**

Systém HSCSD je založen na CSD a je navržen pro vyšší přenos dat pomocí účinnějšího kódování, nižší zpoždění rádiového rozhraní a zároveň je poměrně nákladný a to byl také důvod proč se v síti GSM používala GPRS. U EDGE a UMTS byly datové přenosy ještě vyšší. U UMTS byl systém HSCSD rozšířen o podporu šířky pásma a nízkou latencí paketového připojení. Rychlost závisela na TDMA a upload se pohyboval okolo 14,4 kbit/s, ale u download to bylo 28,8/43,2 kbit/s [24].

1.4.2 **GPRS**

Jak již bylo zmíněno GPRS byla levnější varianta HSCSD. Jedná se o datovou službu, která běží na 2G a 3G mobilních sítích. Původně byl standardizován ETSI, ale nyní se o ní stará 3GPP. Sítě GPRS pracují na principu best-effort, což znamená variabilní propustnost a latenci, která závisí na dalších uživatelích, kteří sdílí službu současně.

Na rozdíl od přepojování okruhů se o kvalitu stará QoS. V sítích 2G jsou přenosové rychlosti od 56 do 114 kbit/s. Sítě GPRS podporují protokoly IP (Internet Protocol), PPP (Point-to-Point) a X.25. Další zařízení, které podporují GPRS jsou rozděleny do tříd A až C. Modulace (resp. klíčování) funguje na GMSK. Sestupný směr u GPRS se pohybuje okolo 64,2 - 85,6 kbit/s [25] [26] [27].

1.4.3 **EDGE/EGPRS**

Při použití dosahujeme lepší ceny za přenos dat pomocí mobilního telefonu a je zpětně kompatibilní se sítí GSM. Toto rozšíření se začlenilo do systému GSM v roce 2003 (nejprve ve Spojených Státech Amerických). EDGE byl vyvinut za pomocí technologie D-AMPS. Díky sofistikovaným metodám kódování a přenosu dat, nám EDGE přináší vyšší přenosové rychlosti na rádiový kanál a tím se ztrojnásobí vzrůst kapacity a výkonu ve srovnání z GSM/GPRS. Systém EDGE/EGPRS je implementován do 2,5G sítích GSM/GPRS. Nadstavba EDGE nevyžaduje žádných hardwarových a softwarových změn, které mají být provedeny v GSM páteřních sítích. Evolved EDGE pokračuje v Release 7 standardu 3GPP, která poskytuje sníženou latenci na polovinu (z 20 ms na 10 ms) a více než zdvojnásobil výkon například u HSPA. Další faktor zvýšení přenosové rychlosti je změna modulace z 32QAM a 16QAM na 8PSK u systému Evolved EDGE. U modulace 8PSK (8 Phase Shift Keying) dochází ke snížení odolnosti vůči rušení, ale jen v případě zhoršených povětrnostních podmínek [25] [28].

1.4.4 **CDMA2000**

Je taky označován jako C2K nebo IMT Multi-Carrier (IMT-MC). Tento systém je vyvíjen 3GPP2 a je zpětně kompatibilní s cdmaOne (IS-95). Používá se zejména v Severní Americe a Jižní Koreji. Je konkurentem UMTS a byl vyvinut společností 3GPP, která se používá v Evropě, Japonsku a Číně. Normy a standardy pro CDMA2000 jsou následující, pro hlas: CDMA2000 1XRTT, 1X Advanced, a pro data: CDMA2000 1xEV-DO (Evolution-Data Optimized): Release0, Revision A, Revision B, Ultra Mobile Broadband (UMB) [29].

1.4.5 **WiDEN**

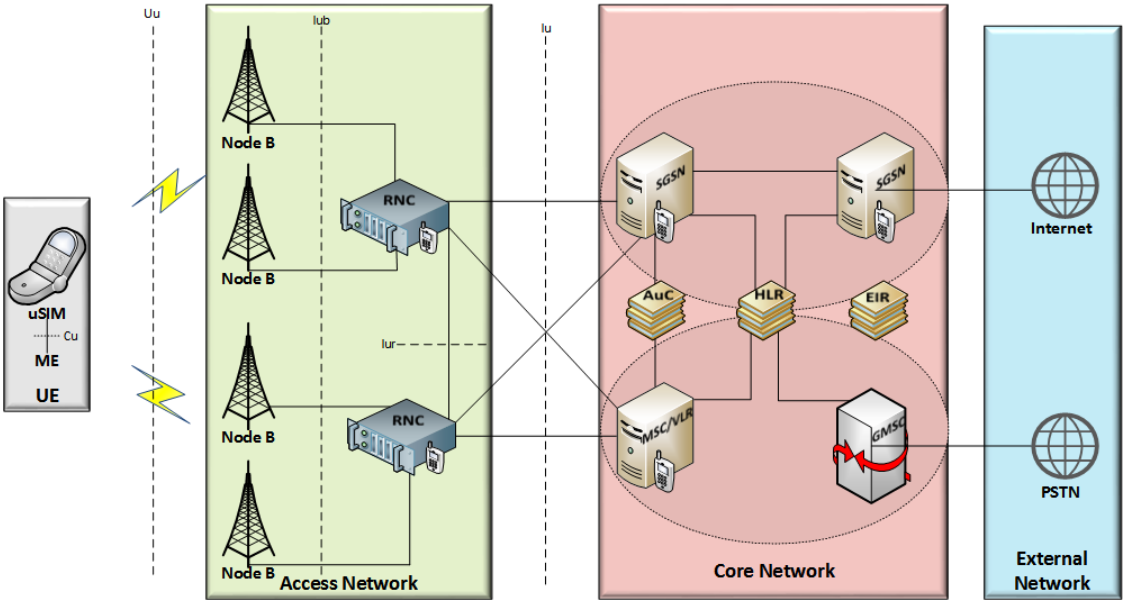
WiDEN (Wideband iDEN) je softwarový upgrade iDEN. Byla představena v roce 1993 společností Motorola a první komerční použití bylo ve Spojených Státech v roce 1996 společností Nextel. Bohužel se komerčně neprosadila kvůli nasazení technologie CDMA. Nextel vypnula WiDEN v roce 2005 a původní technologie iDEN byla z důvodu zavedení LTE vypnuta v roce 2013.

1.5 Sítě třetí generace (3G)

Třetí generace (zkratka 3G někdy taky IMT-2000) zajišťuje služby, které přenáší informace alespoň rychlostí 200 kbit/s. První 3G sítě byly zavedeny v roce 1998 a převážně zaměřeny na datové přenosy [31].

1.5.1 UMTS

Je to mobilní síť třetí generace, která je založena na standardu GSM, kterou vyvinula a udržuje 3GPP. Společnost 3GPP se označuje jako Release ´99 (technologie UMTS) a v současné době je nejnovější verze Release 14 (zaměřena na 5G). Koncept UMTS je velice podobný GMS konceptu s menším rozdílem. Hlavně v popisech jednotlivých částí a celkového zjednodušení. Později se tato technologie dále rozšiřovala a stávala se oblíbenější. Systém UMTS využívá TDMA a W-CDMA (Wideband CDMA), která poskytuje nejrychlejší přenosové rychlosti než u EDGE a to díky kódování a využití šířky pásma. Vývoj UMTS započal v druhé v polovině 80. let organizací ITU. Společnost 3GPP spolupracovala na standardech s organizacemi ETSI, ARIB, TTA, ATIS a CCSA, ale nejvýznamnější organizace které pomohli UMTS byly IETF a IEEE [32] [33].

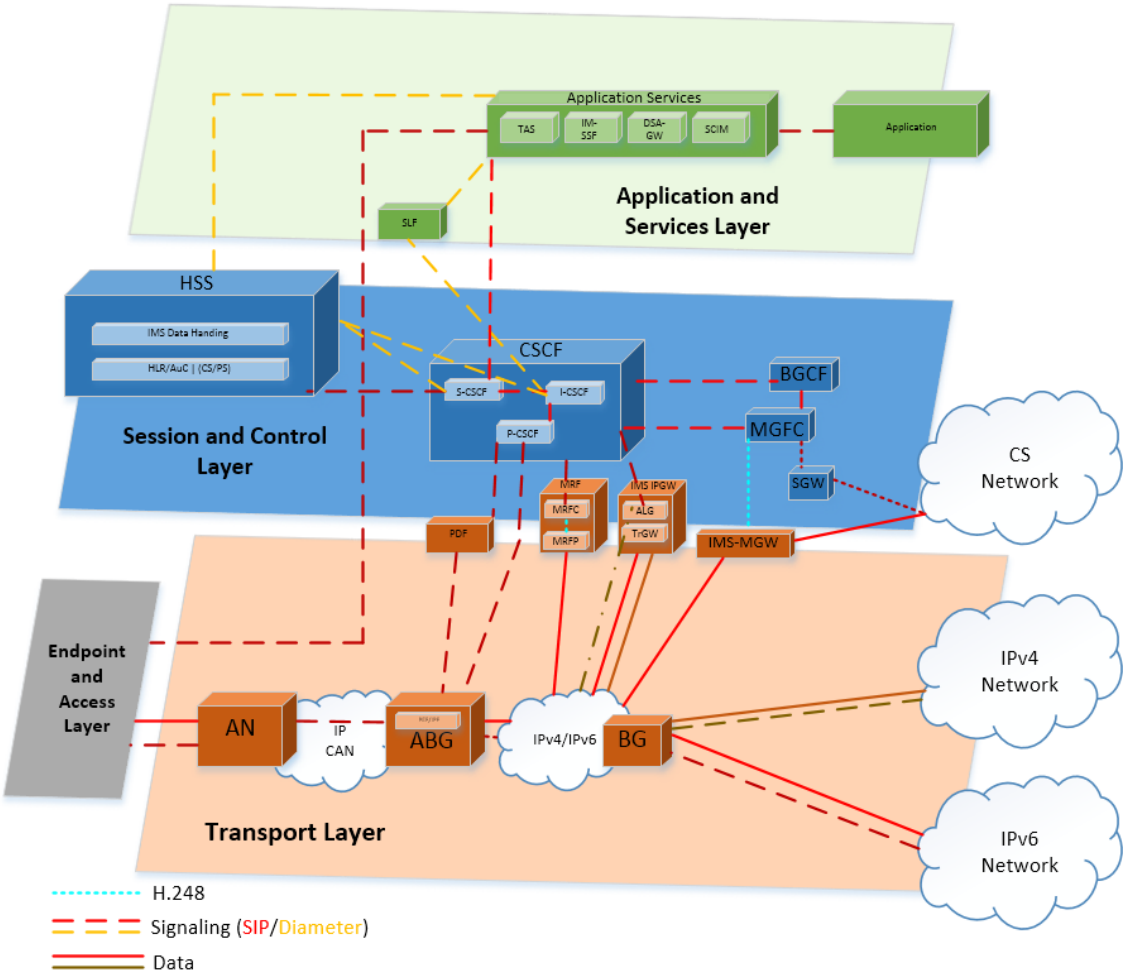


Obrázek 1.1: *Koncept UMTS*

1.5.2 IMS

IMS byla zavedena do UMTS ve verzi Release 4 a 5. Je rozšířením UMTS o multimediální přenosy pomocí přepojování paketů. Zároveň podporuje jak přepojování paketů, tak i přepojování okruhů. Pro IP komunikaci využívá protokolu RTP (Real-time Transport Protocol), RTCP (RTP Control Protocol) a k signalizaci používá protokol SIP (Session Initiation Protocol). Tento model se zachoval i při vytvoření LTE a používá se dodnes. Samotný koncept vznikl v projektu 3GPP a byl navržen tak, že se počítalo s UMTS. Hlavními výhodami IMS je, že pracuje na stávající mobilní infrastruktuře [34] [35] [36] [37].

1.5.3 Koncept IMS



Obrázek 1.2: *Koncept IMS*

Koncept IMS má čtyři vrstvy a to Endpoint and Access Layer, Transport Layer, Session and Control Layer a Application Layer.

1.5.3.1 ***Endpoint and Access Layer***

Endpoint and Access Layer je vrstva, která popisuje zařízení a typ připojení do systému IMS. Pokud se jedná o klasické mobilní telefony, PDA a počítače, tak se mohou registrovat přímo do systému a to i když se jedná o roaming v jiné síti nebo zemi. Je zde ale důležitá podmínka použití IP protokolu ke spuštění agenta SIP. Pokud se jedná o klasické DSL (Digital Subscriber Line), modemy, Ethernet, CDMA2000, W-CDMA, GSM nebo GPRS (EGPRS) bezdrátový přístup WLAN, WiMAX tak i tyto služby ISM podporuje. Ale pokud se jedná o analogové telefony, protokol H.323 které nejsou kompatibilní s IMS, tak se tyto systémy řeší pomocí bran.

1.5.3.2 ***Transport Layer***

Transportní vrstva je jakýsi průsečík mezi vrstvami Endpoint and Access Layer a Control Layer. Je důležité, že nad transportní vrstvou vše běží na bázi IP protokolu, zatím co pod transportní vrstvou to tak být nemusí.

První bránou je MRF (Media Resource Function), je to signalizační uzel, který se chová jako SIP User Agent na S-CSCF a který řídí MRFP (Media Resource Function Processor) s H.248 rozhraním. Zajišťuje (audio/video oznámení) multimediální konference, TTS (Text-to-speech), rozpoznávání řeči a konverzuje mezi různými kodeky.

Druhá brána se označuje IMS-MGW (IMS-Media Gateway, někdy jen MGW). Její úkolem je provádět konverzi médií a transkódování. Z IMS-MGW je připojena přímo na MGFC (Media Gateway Function Controller), který provádí převod řízení hovorů protokolem SIP a ISUP. Prvek MGFC je připojen na SGW (Signalling Gateway) a ten je připojen do PSTN sítě. Brána SGW provádí signalizační konverzi oběma směry a převádí nižší vrstvy protokolu. Brána SGW je připojena k BGCF (Break Out Gateway Control Function), která má za úkol volání z IMS do telefonních sítí (PSTN) pomocí přepojování okruhů a předává zvolené signalizace. Přijímá žádosti relací S-CSCG (nebo jiným BGCF) a vybere síť, ve které je umístěn připojený bod v PSTN. Prvky SGW, MGFC a BGCF se nacházejí v Session and Control Layer.

1.5.3.3 ***Session and Control Layer***

Session and Control Layer je vrstva, která zajišťuje a poskytuje koncovým bodům registrace a směruje SIP signalizační zprávy, které mají být nasměrovány na správný server. Tuto činnost zajišťuje CSCF (Call Session Control Function).

První prvek, který řídí ostatní má označení S-CSCF (Serving-CSCF). Jedná se o centrální uzel, který řídí veškeré relace. Ve své podstatě je to SIP server. Používá Diameter rozhraní do HSS, kde se dají stáhnout uživatelské profily a nahrávat user-to-S-CSCF association. Směrování se provádí pomocí Electronic Numbering lookup (neboli Elektronické číselné vyhledávání). Nadále se stará o registraci uživatele pomocí SIP registrace. A další důležitou částí je Multiple S-CSCFs, které mohou být ve stejné síti a pomáhají rozložit zátěž a zvýšit dostupnost.

Druhý prvek je I-CSCF (Interrogating-CSCF). Jeho hlavní funkce je nalezení HSS pomocí přístupových entit SLF a používá rozhraní Diameter, stejně tak je použit na dotazy HSS a tyto SIP žádosti přesměrovává na S-CSCF. IP adresa I-CSCF je zveřejněna v DNS doménách. Až ve versi Release 7 je možné použít skrytí interní sítě od vnějšího světa (šifrování části zprávy SIP) a je označována zkratkou THIG (Topology Hiding Inter- network Gateway).

Poslední prvek je P-CSCF (Proxy-CSCF), který se stará o přeposílání registračních žádostí od zařízení k I-CSCF (Interrogating-CSCF). Dále pak předává zprávy SIP do S-CSCF, které spravují uživatele, jehož adresa je definována v průběhu registrace a předává žádosti a odpovědi na zařízení. Stará se taky o zabezpečení před možnými útoky a k tomu využívá IPsec, aby chránil soukromí uživatele. Nejčastější útoky jsou typu spoofing. Navíc může obsahovat i PDF (Policy Decision Function) pro opravňování mediálních zdrojů př. QoS.

Další důležitou částí v této vrstvě je HSS. Je to účastnický server, který obsahuje databázi pro IMS. Poskytuje informace o umístění uživatele. Také poskytuje údaje použité pro autentizaci, autorizaci uživatele a dále pak informace používané servisní vrstvou. Také poskytuje klasickou HLR (Home Location Register) a AuC (Authentication Centre) a to umožňuje uživatelům přistupovat k doméně pomocí paketů prostřednictvím IMSI ověření. Uživatelský profil se skládá z identity uživatele, S-CSCF názvu, registrační informace a roaming, parametry autentizace, řídící a informační servis.

1.5.3.4 ***Aplication Layer***

Na poslední vrstvě se nachází několik serverů, které se starají o celkový chod IMS. První server je označen TAS (Telephony Application Server), je SIP uživatelský agent, který udržuje stav volání, poskytuje základy pro volání včetně číselné analýzy, směrování a nastavování hovorů, přesměrování hovorů, atd. Druhý server je IM-SSF (IP Multimedia - Service Switching Function), poskytuje komunikaci propojených SIP zpráv do odpovídající zákaznické aplikace. Pak může zde být doplněk Supplemental Telephony Application Server, který poskytuje doplňkové telefonní služby. Další server v aplikační vrstvě je označen OSA-GW (Open Service Access - Gateway), převádí SIP na Parlay API a poskytuje se pro službu OSA-GW (Open Services Access - Gateway), která je součástí aplikační vrstvy v architektuře 3GPP IMS.

1.6 Sítě přechodové třetí generace (3,5G - 3,75G - 3,9G)

Technologie patřící do třetí přechodové generace jsou zaměřeny čistě na datový provoz a pomoci účastníkům lépe využívat tyto služby. Zároveň jsou připravovány na technologii LTE.

1.6.1 HSPA

Tato nadstavba vylepšuje přenosové vlastnosti u datových přenosů na stávajících 3G mobilních sítích, které využívají WCDMA (jak FDD, tak i TDD) a vznikla sloučením HUSPA

(High Speed Uplink Packet Access) a HSDPA (High Speed Downlink Packet Access). Byla definovaná v Release ´99 a Release 4 (hlavně transportní kanály), ale modifikace přišly v Release 5 a 6. Nejdůležitější protokol je CQI (Channel Quality Indicator), který využívá zbývající výkon v buňce (nový parametr SINR (Signal to Interference plus Noise Ratio)) [33] [37].

1.6.1.1 ***HSDPA***

Jak již bylo zmíněno, toto vylepšení bylo definováno organizací 3GPP v Release 5. Hlavně se jedná o směr sestupný, který pomáhá základovým stanicím lépe zacházet s pakety. Nejdůležitější protokol je HARQ, který dokáže korekci chyb a automatické opakovaní bloků, dokud nejsou doručeny správně. Jejím hlavním cílem je zefektivnit i dostupné přenosové rychlosti rádiového kanálu, pokud nastane chyba. Dalším je Fast Packet Scheduling, který pomáhá rozvrhovat a plánovat přenosové prostředky mezi uživateli a jeho jádro má označení Scheduller a nachází se v NodeB. Další zlepšení nastalo jak v modulaci (16-QAM a 64-QAM), tak přechod na nový anténní systém MIMO. Přenosová rychlost se zlepšila ze 128 kbit/s na 384 kbit/s [33] [37].

1.6.1.2 ***HSUPA***

Je definována organizací 3GPP v Release 6. V podstatě se využily parametry zlepšení z HSDPA a aplikovaly se do HSUPA, aby zlepšení došlo jak v sestupném tak i vzestupném směru [33] [37].

1.6.1.3 ***Evolved HSPA***

Někdy se tato technologie označuje HSPA+. Toto vylepšení bylo standardizováno 3GPP v Release 7 až do 10. Je srovnatelná s technologií LTE. Poskytuje přenosovou rychlost 56 Mbit/s ve směru sestupném (64-QAM) a 22 Mbit/s ve směru vzestupném (16-QAM). Založena na modulaci OFDM a vícenásobného přístupu. Toto rozšíření bylo nasazeno pro snadnou integraci systému LTE, proto je označena jako 3,9G technologie [37].

1.6.2 **Mobile WiMAX (802.16e)**

WiMAX (Worldwide Interoperability for Microwave Access) je bezdrátová komunikace, která dosahuje rychlostí 30 až 40 Mbit/s a po roce 2011 rychlost narostla na 1 Gbit/s. Založení této technologie započalo v roce 2001. Technologii WiMAX se nakonec nepodařilo dosáhnout dominance na trhu kvůli problémům s celkovým počtem připojených uživatelů. Na jednu anténu se mohlo připojit maximálně 8 uživatelů, aby byla zaručena rychlost, kterou WiMAX uvádí. Pokud se připojilo více uživatelů na anténu tak se rychlost razantně snížila. WiMAX je z rodiny IEEE 802.16 a 802.11 [38].

1.7 Sítě čtvrtá generace (4G)

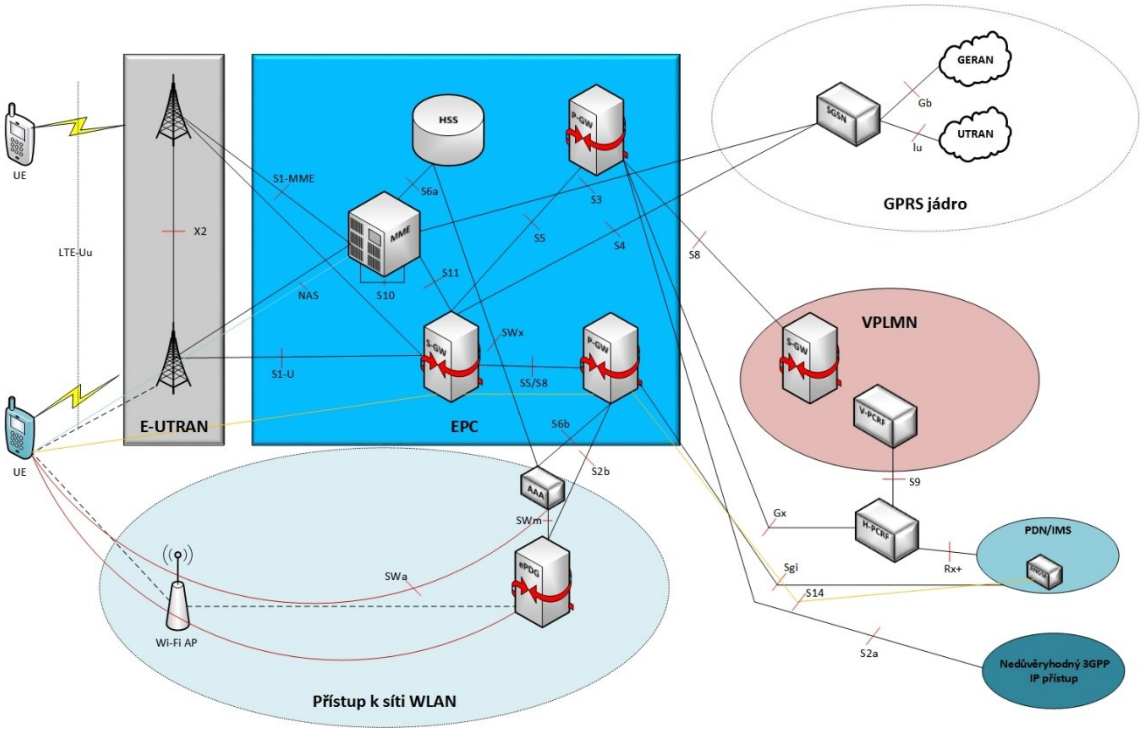
Čtvrtá generace přináší celkové zrychlení datových přenosů podle IMT Advanced, které definují ITU a teoreticky by měla rychlost přenosu dosahovat až 1 Gbit/s / 500 Mbit/s. Hlavní technologií v této generaci je LTE i když ta stále nesplňovala požadavky na 4G a LTE+ která je již řazena do 4G technologie. Mobilní zařízení, které se dostávají na trh, mají již zabudovanou podporu 4G a jsou schopny při zapnutí datového připojení se připojit na tuto síť.

1.7.1 LTE

Jak již bylo zmíněno, LTE je řazena do 3,9G nikoli do 4G z důvodu nesplnění požadavků ITU pro 4G sítě. LTE je definována standardem organizací 3GPP v Release 8 a 9. První návrh na tuto síť vznikl v roce 2004 a první testování LTE proběhlo v roce 2008 (Release 8). Na rozdíl od předchozích technologií, které zastřešoval projekt 3GPP, LTE vyvinula Japonská společnost NTT DoCoMo. Mezi hlavní výhody LTE je vysoká propustnost jak v sestupném tak i vzestupném směru (pro sestupný směr OFDM 100Mbit/s a pro vzestupný směr SC-FDMA 50 Mbit/s). Další nespornou výhodou je nízké zpoždění (čas kdy se zařízení dokáže připojit do sítě), navíc dokáže využívat jak FDD, tak i TDD což umožňuje kompatibilitu se sítěmi předešlé generace. S tím souvisí i jednoduchá architektura, která nemá tak vysoké provozní náklady, protože je postavena na bázi IP protokolu a to včetně základových stanic (eNodeB). S touto architekturou bylo standardizováno i QoS, aby se na všech rozhraních zajistila vysoká kvalita hlasového volání za jakýchkoli okolností. S tím souvisí i škálovatelnost šířky pásma, která mohou být od 1.4, 3, 5, 10, 15 a 20 MHz. Těmito vlastnostmi se jeví LTE atraktivním jak pro operátory, tak i pro odběratele. A také se díky jednoduchosti vyvíjejí projekty, které jsou na bázi otevřeného zdrojového kódu. Jedním z nich je projekt openLTE. Navíc lze veškerou dokumentaci a popisy najít na webových stránkách organizace 3GPP [39] [40] [41] [42] [43] [44] [45] [49].

1.7.1.1 ***Koncept LTE***

Architektura LTE je označována LTE/SAE (System Architecture Evolution). Cílem je zvládnout datový provoz efektivně z hlediska výkonu a nákladů. Dále pak je možnost oddělit uživatelská data a signalizace, díky které mohou operátoři dimenzovat a přizpůsobovat snadno své sítě.



Obrázek 1.3: *Koncept LTE*

Každé UE je připojeno k jednotlivým eNodeB a rozhraní mezi nimi má označení LTE-Uu. Samotné základové stanice eNodeB, jsou vzájemně propojeny a komunikují přes rozhraní X2 (E-UTRAN) a následně je každé eNodeB připojeno do jádra sítě EPC pomocí rozhraní S1-(MME/U). Pokud se bavíme o rozhraní S1-MME, tak je přímo základová stanice připojena na MME, zatímco rozhraní S1-U je připojeno přímo na S-GW. Nyní se blíže podíváme na jádro celé architektury LTE, která má označení EPC (Evolved Packet Core):

- Brána S-GW (Serving Gateway) je přímo připojena ke každé eNodeB pomocí rozhraní S1-U. Jedná se o odrazový můstek kam se připojit. Může se přes rozhraní S11 připojit do MEE, nebo pokud se potřebujeme dostat do jiné sítě např. do GPRS Core, tak to lze pomocí rozhraní S4 a pokud někde mimo síť, tak to lze přes rozhraní S5/S8 do P-GW, která nás přepojí dál, kam potřebujeme.
- MME (Mobility Management Entity) má na starost signalizace mezi uživatelem a jádrem sítě, které se týkají mobility a bezpečnosti pro eNodeB přístup. Skenuje UE v klidovém režimu a NAS zprávy. Stará se o veškeré procedury, které se týkají správného chodu celého systému (autentizace, autorizace, bezpečný přenos přenášených dat, aj.).
- HSS je databáze, která obsahuje uživatelské informace. Poskytuje také podpůrné funkce v oblasti řízení mobility. Tato součást se dochovala již z 2G (GSM) s tím rozdílem že registry HLR a AuC jsou spojeny dohromady. HSS je spojena s MME pomocí rozhraní S6a.

- P-GW (PDN Gateway) její hlavní úlohou je filtrování paketů pro každého uživatele, kvalita služby, řízení datového toku, podpora nabíjení, odposlouchávání a třídění paketů. Slouží jako odrazový můstek pro připojení do 3GPP technologií (rozhraní Sgi, S14, S8, Gx) nebo nepatří do 3GPP/3GPP2 technologií (př. WiMAX) rozhraní S2a.

Další významné části jsou:

- H-PCRF (Policy Control and Charging Rules Function) jedná se funkci, která definuje politiku a regulační rozhodnutí. Konkrétně se jedná o protokol QoS, který koordinuje mezi externí PDN/IMS a EPC. Vynucuje minimální parametry QoS pro pakety na základě jejich QoS parametrů a určuje, jak by se měly pakety účtovat (Charging Policy), dynamicky řídit a kontroluje datové relace. Nachází se mezi P-GW a PDN/IMS a to buď přímo přes rozhraní SGi, nebo přes rozhraní Gx do H-PCRF a přes rozhraní Rx+ do PDN/IMS.
- ANDSF (Access Network Discovery and Selection Function) její hlavní úlohou je zjistit, jestli zařízení je kompatibilní do 3GPP mobilní sítě či nikoli. Zařízení, které dokáží být použity pro datovou komunikaci a zároveň nejsou v partnerském projektu 3GPP (WiMAX, Wi-Fi, aj.). ANDSF komunikuje s UE pomocí rozhraní S14.

Přístup k síti WLAN je další možnost, jak přistoupit do sítě LTE přes zařízení, které je nedůvěryhodné do 3GPP technologie. Takto vytvořené spojení se uskuteční přes ePDG, který tvoří tunel pomocí IPsec protokolu. Následně je mezi ePDG a P-GW vytvořen GRE tunel, který umožní bezpečné připojení do internetu. K tomuto účelu slouží rozhraní SWa, SWm, SWx, pak S6b/S2b připojení k P-GW. Mobilní operátor T-Mobile nabízí tento přístup pro telefonní zařízení iPhone 5 a vyšší a pro telefonní zařízení Samsung Galaxy S6 a S7.

1.7.2 **LTE Advanced**

Je vylepšená verze LTE a je hlavním kandidátem 4G systému. Standardizován byl v roce 2011 projektem 3GPP v Release 10. Samotný formát navrhovala společnost NTT DoCoMo a později se stal mezinárodním standardem. První testování proběhlo ve Švédsku a Norsku v roce 2009. Spojené Státy Americké a Japonsko prováděly testy v roce 2010. Po opravách a vylepšeních LTE mohla být LTE+ prohlášena za 4G technologii. První testování LTE+ v České Republice bylo spuštěno v Praze v roce 2014 společností O2. Došlo ke zvýšení přenosu dat ve směru sestupném na 3 Gbit/s a ve směru vzestupném na 1,5 Gbit/s. Bylo dosaženo vyšší spektrální účinnosti, zvýšení počtu aktivních účastníků a zlepšený výkon v buňkách. Mezi nové funkce patří CA (Carrier Aggregation), podpora RN (Relay Nodes)a lepší využití MIMO antén. Další verze LTE, které se připravují od Release 11 mají označení LTE-B, LTE-C [46] [43].

2 USRP a open-source projekt GNU Radio

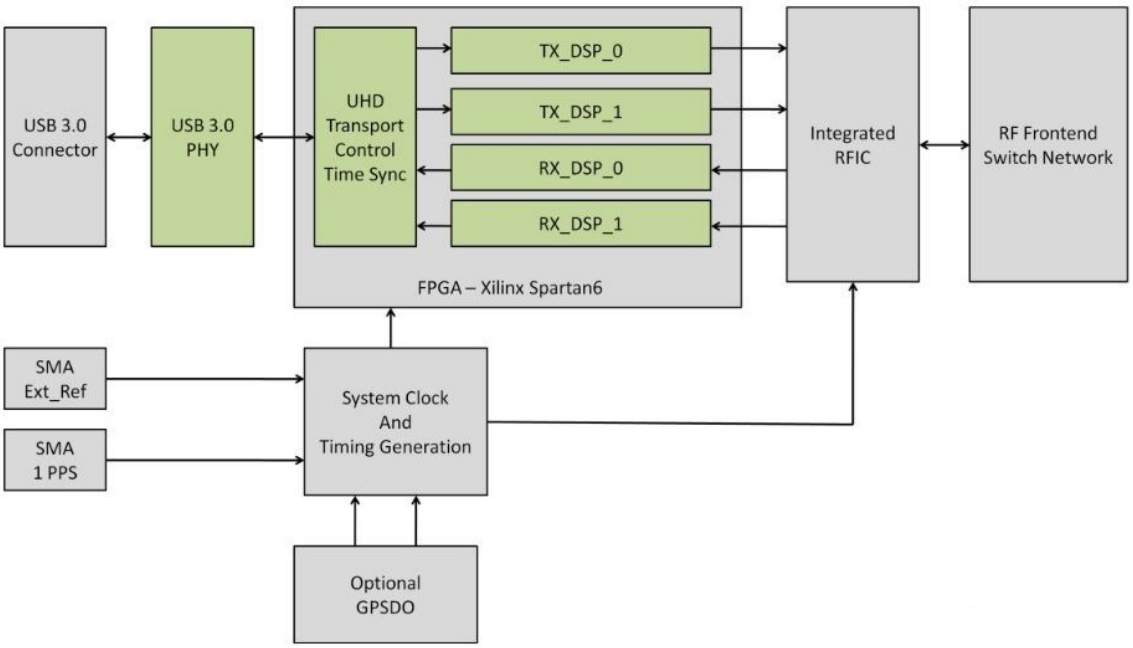
2.1 USRP

První SDR (Software Defined Radio) byl poprvé uskutečněn v roce 1991 Josephem Mittolou. Ten na kus papíru publikoval svůj nápad v roce 1992. O čtyři roky později vzniklo první SDR fórum a skládalo se z lidí a organizací. Protože do poloviny roku 2000 nikdo nedokázal prosadit nápad s SDR, tak se v roce 2004 rozhodl Matt Ettus založit společnost, kterou pojmenoval Ettus Research a s jeho týmem se mu povedlo poprvé zrealizovat první USRP. Používá open-source GNU Radio a komerčně dostupný hardware, který je cenově přijatelný. Tyto produkty začaly hojně využívat ve výzkumu, ve školách, amatérští fanoušci, hackeři, ti všichni si tento produkt oblíbili. Velké obchodní společnosti dokonce budovaly komplexnější sítě pomocí USRP. Nejen že se rozšířila oblíbenost, ale i komunita, která pomáhá udržovat a vylepšovat software pro hardware USRP. USRP a GNU Radio poskytují jednoduchý model a programovatelné hradlové pole. V roce 2010 se společnost Ettus Research rozhodla ke strategickému kroku, který má pomoci zákazníkům získat větší potenciál z SDR a došlo ke spojení se společnosti NI (National Instrument). Samozřejmě že Ettus Research nadále funguje nezávisle na NI a podporuje open-source komunitu. Společnost NI zavedla nejnáročnější aspekt ve vývoji SDR software. Zavedením NI USRP RIO pro náročnější aplikace, které jsou nákladné, dříve obtížné, nebo nedosažitelné jsou nyní možné s programem LabVIEW. I společnost MathWork podporuje USRP B200/B210/X300/X310 s verzí R2014b. Za pomocí software Simulink můžeme zajistit, že údaje získané z rádia zpracujeme v reálném čase. Nyní se podíváme na produkt USRP B2X0. V současné době je kromě desky USRP možnost zakoupit desky HackRF nebo bladeRF [47] [54].

2.1.1 USRP B2x0

Tato série má integrované RF, které jsou schopny pracovat ve frekvenčním rozsahu od 70 MHz do 6 GHz. Dále pak jeden PPS vstup a jeden pro 10 MHz. Konfigurovatelnou taktovací frekvenci, variabilní šířku pásma od 200 kHz do 56 MHz, GPIO hlavičku (B200/B210 má interní GPSDO možnost). Naopak B210/B200mini mají i JTAG konektor a pouze B210 MICRO Debug konektor. Ve většině případů má (kromě B100) externí napájení USB 3.0 (duálně A, micro-B nebo B), který musí být použit. Každé zařízení potřebuje ovladač pro komunikaci mezi počítačem a USRP produktem. Tyto ovladače mají označení UHD, které nám umožní pracovat s touto deskou. Jsou open-source a dnes je již možnost je získat i pro jiné operační systémy než je Linux. Jak již bylo zmíněno, nejen že komunita je ochotná pomoci, ale můžeme se sami zapojit a pomáhat vylepšovat software pro tyto produkty. Na základní desce je FPGA typu Xilinx Spartan 6 XC6SLX75/150 (pro B200 75 a pro B210 150). B210 má zabudovaný nový anténní systém 2x2 MIMO, což B200 nemá. V obou případech zvládnou half nebo full-duplex. Modulárnost této desky lze využít pro připojování zásuvných modulů "daughterboard" pro rozšíření. Antény, které je nutné dokoupit lze připojit pomocí SMA-SMA

kabelu, nebo našroubovat do příslušného konektoru. USRP B2X0 jsou stále v nabídce. Balení obsahuje sérii BUS což je pouze základní deska s napájecím kabelem a USB 3.0.



Obrázek 2.1: *Blokové schéma USRP B2x0*

Další produkty od této společnosti jsou rozděleny do různých kategorií produkty B2X0 patří do série (Bus série). Produkty X3x0 (X série), N2x0 (Network série), E310 (Embedded série), přídavné moduly (Daughterboards), antény, kabely a příslušenství.

2.2 GNU Radio

Vznik tohoto projektu započal v roce 2001, který zainvestoval John Gilmore. Vedoucím projektu a zároveň hlavním programátorem se stal Eric Blossom. Z pohledu softwaru docházelo ke stálému zlepšování, až se skutečně povedlo vytvořit program, který dokáže simulovat přenos pro zpracování signálů. Problém byl pouze v hardwarové části a tu vyřešil Matt Ettus se svým týmem a společností Ettus Research, který se připojil do týmu GNU Radio. Díky němu a jeho týmu se povedlo zcela realizovat a využít potenciál SDR. V roce 2010 Eric Blossom odstoupil z čela projektu a novým projektovým manažerem se stal Tom Rondeauvi. Projekt GNU Radio je open-source software, který je plně zdarma a bloky slouží pro zpracování signálu k implementaci softwaru s rádiem. Aby se toho dosáhlo, člověk si může zvolit simulaci v GNU Radio Companion, nebo pořídit cenově dostupný hardware s externím RF a vytvářet projekty. Díky těmto vlastnostem se projekt GNU Radio rozšířil nejen pro fanoušky, ale začalo se využívat i na akademických půdách (diplomové, bakalářské práce), tak i v komerční sféře, aby podpořili bezdrátový výzkum. V současné době je plně funkční na operačních systémech Linux, Windows a MAC. Projekt GNU Radio má obrovskou komunitu, která pomáhá odhalovat chyby a udržovat celý projekt v chodu. Projekt je postaven tak, aby uživatel mohl bloky nejen

propojovat, ale pokud některý z bloků chybí tak ho lze snadno vytvořit a přidat. Celá aplikace je psána v jazyce Python, zatím co samotné zpracování signálu je implementováno v jazyce C++. V roce 2014 GNU Radio spustilo nový projekt PyBOMBS (Python Build Overlay Managed Bundle System) a v roce 2015 byla k dispozici první verze, která umožňuje zřizovat závislosti v projektech out-of-tree [51] [52] [53].

3 Návrh a praktická realizace prvku eNodeB pomocí openLTE.

V kapitole tři postupně popisuji, jak si vytvořit vlastní přístupový bod eNodeB pomocí otevřeného zdrojového kódu openLTE. Než začneme provádět kroky ke spuštění, je nutné použít stíněné prostory proti rušení, aby se nestalo, že po spuštění budeme překrývat frekvenční pásmo operátorů. Následně je nutné mít počítač s operačním systémem Linux a softwarově definované rádio, které nám pomůže vybudovat přístupový bod eNodeB. Hlavním bodem diplomové práce bylo ověření reálné použitelnosti projektu openLTE.

3.1 Použité komponenty

Komponenty pro praktickou část byly následující:

- Počítač (Operační systém: Linux Mint 16 Petra Ciannamon-64bit/Windows 7 x32
  Hardware: Intel Core i7, 4GB RAM, NVIDIA GeForce 8400 GS, 2x USB 3.0, 8x USB 2.0)
- SDR: USRP B210 (2x externí anténa, 1x USB 3.0 kabel, externí napájení)
- Programovatelné uSIM katry (typ Milenage 3x)
- Zařízení na programování uSIM karet (Blutronics Bludrive II CCID)
- 3x mobilní zařízení s podporou 4G (LG G3, Sony Xperia V, BlackBerry Z10)

3.2 Upgrade Linux Mint

Počítač, na kterém byla provedena praktická část, byl s instalovaným operačním systémem Linux Mint 16 Petra Cinnamon 64-bit (Ubuntu Core 13.10) a Windows 7 x32. Před instalacemi balíčků byl nutný test ve Virtualboxu a zjistit, jestli bude možné balíčky stáhnout na aktuální verzi systému. Z důvodu, že byla ukončena podpora Mint 16, ale také na danou verzi byla ukončena podpora potřebných balíčků, bylo nutné provést instalaci na vyšší verzi a to 17.3 Rosa Cinnamon 64-bit (Ubuntu Core 14.04). Postup byl následující:

1) Nejprve byly provedeny zálohy:

```
sudo cp /etc/apt/sources.list /etc/apt/sources.list.bak

sudo cp /etc/apt/sources.list.d/official-package-
repositories.list /etc/apt/sources.list.d/official-package-
repositories.list.bak

sudo cp /etc/apt/sources.list.d/official-source-
repositories.list /etc/apt/sources.list.d/official-source-
repositories.list.bak
```

2) Přepsání source list:

```
sudo sed -i 's/saucy/trusty/' /etc/apt/sources.list
sudo sed -i 's/petra/qiana/' /etc/apt/sources.list
sudo sed -i 's/saucy/trusty/'
/etc/apt/sources.list.d/official-package-repositories.list
sudo sed -i 's/petra/qiana/'
/etc/apt/sources.list.d/official-package-repositories.list
```

3) Poté provedeme instalaci aktualizačních balíčků:

```
sudo apt-get update
```

4) Upgrade na verzi Mint 17 Ciannomode-64bit:

```
sudo apt-get dist-upgrade
```

5) Provedeme restart:

```
sudo reboot
```

Po těchto krocích se povedlo načíst operační systém ve verzi 17.0 a následně v Software Manager bylo možné naistalovat verzi 17.3 Rosa. Po tomto kroku byl znovu restartován systém a získali jsme aktuální verzi systému 17.3. V tomto případě bylo zaznamenáno, že proces byl v chodu po dobu čtyř hodin z důvodu rychlosti stahování 17,6 kbit/s.

3.3 Instalace balíčků

Před kompilací je nutné stáhnout a naistalovat balíčky, které pomohou k chodu projektu openLTE. Jelikož openLTE je závislá na projektu GNU Radio a ovladači UHD je třeba ověřit, zda jsou všechny balíčky naistalovány a aktuální. Proto navštívíme webovou stránku GNU Radio, která má veškeré informace, které pomohou při kompilaci. Zde je seznam balíčků, které byly použity [55]:

```
sudo apt-get install
libusb-1.0-0-dev doxygen python-mako python-docutils cmake
build-essential git-core git g++ python-dev swig pkg-config
libfftw3-dev libboost1.55-all-dev libcppunit-dev libgsl0-
dev libusb-dev libsdl1.2-dev python-wxgtk2.8 python-numpy
python-cheetah python-lxml libxi-dev libqt4-opengl-dev
libqwt-dev libfontconfig1-dev libxrender-dev python-sip
python-sip-dev ccache guile-2.0 sdcc alsa-base libasound2
libasound2-dev python-qt4 python-qwt5-qt4 libqt4-opengl-dev
libqwt5-qt4-dev libxi-dev libsdl1.2-dev python-pip
```

Dále jsou zde uvedeny balíčky, u kterých byla nalezena chyba v kompilaci:

```
libboost-all-dev libuhd-dev libuhd003 uhd-host
```

`libboost-all-dev` – je nekompatibilní s GNU Radiem v novějších verzích.

`libuhd-dev, libuhd003 a uhd-host` – jsou doporučené z Ettarus Research. Po instalaci těchto tří, nebo jednoho z nich se stane, že se kompilace ukončí v 85% s chybovou hláškou.

Po instalaci byl proveden update/upgrade a přejdeme k samotné kompilaci.

Tento krok není povinný, ale pro svou práci jsem si ho zvolil. Do bashrc jsem nastavil cesty pro GNU Radio (při kompilování by se cesty, měli navolit sami):

```
export PATH=$PATH:/opt/gnuradio/bin
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/gnuradio/lib
export
PKG_CONFIG_PATH=$PKG_CONFIG_PATH:/opt/gnuradio/lib/pkgconfig
export PYTHONPATH=$PYTHONPATH:/opt/gnuradio/lib/python2.6/site-
packages
```

3.4 Kompilace GNU Radio

Kompilace GNU Radia jsou tři. Nejednoduší způsob je použití skriptu, druhý způsob je kompilovat pomocí projektu PyBOMBS a nejtěžším způsobem je kompilovat vše manuálně. V této části jsem využil kompilaci pomocí skriptu. Jeho hlavní výhodou je, že se stáhne vše, co bude potřeba ke zprovoznění přístupového bodu. Nejen GNU Radio (nejnovější verze), ale také ovladače k USRP (UHD). Kroky jsou následující [56]:

1) Nejprve vytvoříme novou složku, do které se budou stahovat potřebné soubory:

```
sudo mkdir gnuradio
cd gnuradio
```

2) Potom příkazem stáhneme skript:

```
wget http://www.sbrac.org/files/build-gnuradio
```

Po stáhnutí skriptu je nutné provést úpravu editorem (gedit), protože některé balíčky již neexistují. Konkrétně `libzmq a libzmq1-dev` a naopak balíčky `libzmq-dev a libzmq1` jsou nutné.

3) Po stáhnutí a úpravě nastavíme práva:

```
chmod a+x ./build-gnuradio
```

4) Po předchozím kroku se stal soubor spustitelný a příkazem se provede kompilování.

```
./build-gnuradio -v
```

U vytváření složky se použije sudo, ale v dalších krocích (kromě změn ve skriptu) se sudo nepoužívá, protože byly zaznamenány problémy. Po spuštění se zahájí kompilace, která trvá přibližně 2 hodiny. Skript lze spustit s parametrem –v. Ten bude detailně vypisovat stav kompilace.

Při spuštění skriptu vás upozorní, že je nutné mít větší místo na disku než je 500 MB. Z osobní zkušenosti doporučuji mít minimálně 2GB místa, protože nestahujeme jen ovladače na USRP a GNU Radio, ale i jiné potřebné soubory.

```
**************************************************************
You should probably set your PYTHONPATH to:

    /usr/local/lib/python2.7/dist-packages

Using:

export PYTHONPATH=/usr/local/lib/python2.7/dist-packages

in your .bashrc or equivalent file prior to attempting to run
any Gnu Radio applications or Gnu Radio Companion.
**************************************************************
Done function pythonpath at: St bře 2 14:35:13 CET 2016
Starting function extras at: St bře 2 14:35:13 CET 2016
Done function extras at: St bře 2 14:35:13 CET 2016
Done all functions at: St bře 2 14:35:13 CET 2016
All Done

========================================================================
If you have found this script useful and time-saving, consider a
donation to help me keep build-gnuradio, simple_ra, SIDsuite,
meteor_detector, simple_fm_rcv, and multimode maintained and up to date.
A simple paypal transfer to mleech@ripnet.com is all you need to do.
========================================================================
Send success/fail info to sbrac.org?
```

Obrázek 3.1: *Úspěšná kompilace GNU Radio*

Po ukončení kompilace ověříme příkazem verzi GNU Radio:

```
gnuradio-config-info -v
```

Verze GNU Radio 3.7.9.1 a provedeme test funkčnosti USRP B210 příkazem [59]:

```
uhd_usrp_probe
```

```
linux; GNU C++ version 4.8.4; Boost_105500; UHD_003.010.git-156-g2d68f228

-- Loading firmware image: /usr/local/share/uhd/images/usrp_b200_fw.hex...
-- Detected Device: B210
-- Loading FPGA image: /usr/local/share/uhd/images/usrp_b210_fpga.bin... done
-- Operating over USB 3.
-- Detecting internal GPSDO.... No GPSDO found
-- Initialize CODEC control...
-- Initialize Radio control...
-- Performing register loopback test... pass
-- Performing register loopback test... pass
-- Performing CODEC loopback test... pass
-- Performing CODEC loopback test... pass
-- Setting master clock rate selection to 'automatic'.
-- Asking for clock rate 16.000000 MHz...
-- Actually got clock rate 16.000000 MHz.
-- Performing timer loopback test... pass
-- Performing timer loopback test... pass
 _____________________________________________
/
|       Device: B-Series Device
|     _____________________________________
|    /
```

Obrázek 3.2: *Nahrání firmware a FPGA na SDR*

Příkaz `uhd_find_device` slouží pro vyhledávání USRP zařízení, které jsou připojeny k počítači [58].

3.5 openLTE

Projekt openLTE vznikl v roce 2011. Založil ho Ben Wojtowicz a první verze byla 00.01, která uměla jen sestupný přenos a příjem. V současné době je aktuální verze 19.04. Projekt je stále ve verzi alfa. Všechny informace a soubory ke stažení jsou dostupné ze stránek sourceforge.net. V tomto projektu se snaží vývojáři implementovat specifikace z 3GPP, která standardizuje LTE.

Pro zajištění chodu je nutné mít softwarově definované rádio USRP B2x0, Blade RF nebo HackRF. Pak komponenty GNU Radio, GrOsmoSDR, rtl-sdr, UHD, polarssl, iptables [57].

Ještě před samotnou kompilací je nutné stáhnout balíček polarssl:

```
sudo apt-get install libpolarssl-dev
```

1) Stáhneme z webové stránky sourceforge.net projekt openLTE:

```
https://sourceforge.net/projects/openlte/files/openlte_v00-19-02.tgz/download
```

2) Příkazem rozbalíme stažený soubor:

```
sudo tar xzf openlte_v00-19-02.tgz
```

3) Vytvoříme novou složku, kde bude probíhat kompilace projektu openLTE:

```
sudo mkdir build
```

4) Provedeme kompilaci:

```
sudo cmake ../

sudo make

sudo make install
```

```
Install the project...
-- Install configuration: "Release"
-- Up-to-date: /usr/local/lib/libLTE_fdd_dl_fg.so
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fg/_LTE_fdd_dl_fg.so
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fg/LTE_fdd_dl_fg.py
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fg/LTE_fdd_dl_fg.pyc
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fg/LTE_fdd_dl_fg.pyo
-- Up-to-date: /usr/local/include/LTE_fdd_dl_fg/swig/LTE_fdd_dl_fg.i
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fg/__init__.py
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fg/__init__.pyc
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fg/__init__.pyo
-- Up-to-date: /usr/local/bin/LTE_fdd_dl_file_gen.py
-- Up-to-date: /usr/local/lib/libLTE_fdd_dl_fs.so
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fs/_LTE_fdd_dl_fs.so
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fs/LTE_fdd_dl_fs.py
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fs/LTE_fdd_dl_fs.pyc
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fs/LTE_fdd_dl_fs.pyo
-- Up-to-date: /usr/local/include/LTE_fdd_dl_fs/swig/LTE_fdd_dl_fs.i
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fs/__init__.py
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fs/__init__.pyc
-- Up-to-date: /usr/local/lib/python2.7/dist-packages/LTE_fdd_dl_fs/__init__.pyo
-- Up-to-date: /usr/local/bin/LTE_fdd_dl_file_scan.py
-- Up-to-date: /usr/local/bin/LTE_fdd_dl_scan
-- Up-to-date: /usr/local/bin/LTE_file_recorder
-- Up-to-date: /usr/local/bin/LTE_fdd_enodeb
```

Obrázek 3.3: *Úspěšná kompilace openLTE*

Celkový čas pro tuto operaci je asi 3-4 minuty.

3.6 Příprava před spuštěním

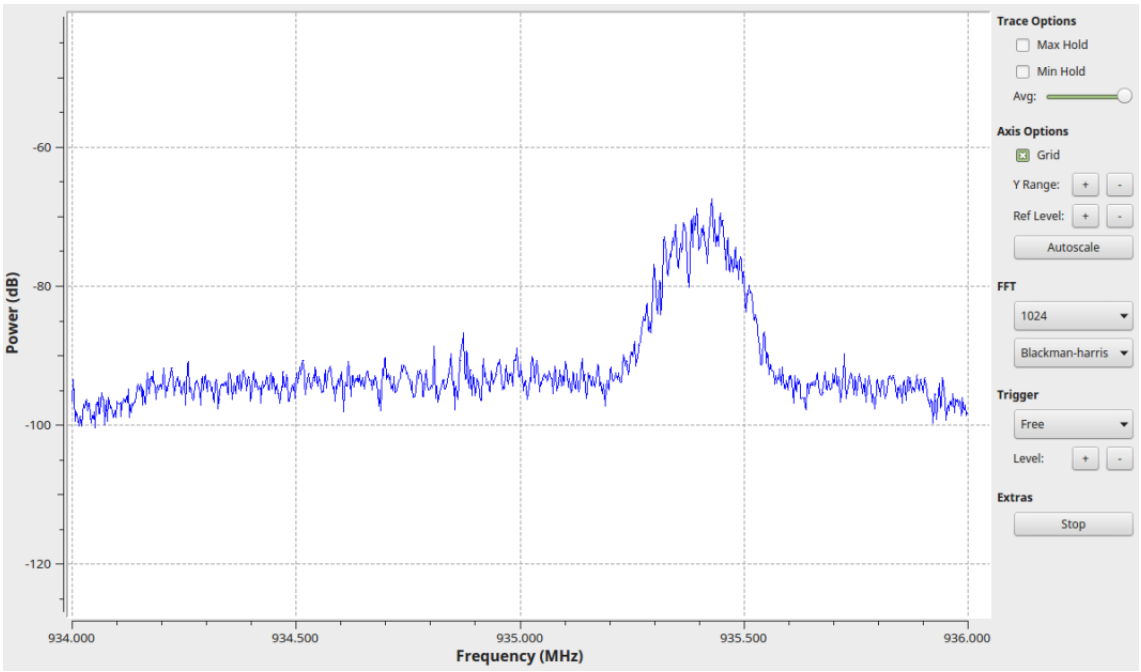
Před zahájením spuštění musíme vyhledat LTE pásma, které využívají čeští mobilní operátoři. Dále je důležité vyhledat informace, v kterých pásmech pracují mobilní zařízení. V České republice se využívají pásma 1, 3, 7, 8 a 20. Důrazně doporučuji využít odstíněné prostory, aby nedocházelo k narušování do pásem mobilních operátorů. Pokud toto místo nemáme, musíme využít spektrální analyzátor a zjistit, kde se dá vybudovat náš přístupový bod.

Příklady jak použít USRP na prohledávání spektra:

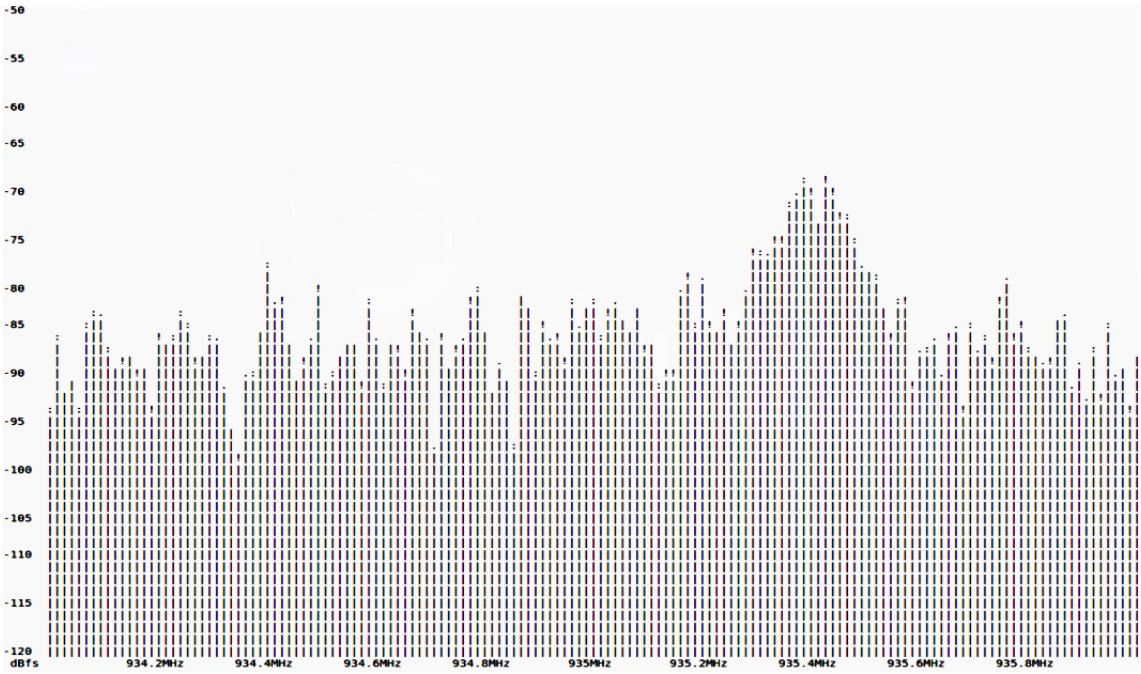
```
uhd_fft
```

nebo ve složce /gnuradio/uhd/build/examples použít soubor, který provede spektrální analýzu přímo v terminálovém okně:

```
rx_ascii_art_dft
```



Obrázek 3.4: *Spektrální analýza (s využitím UHD FFT)*



Obrázek 3.5: *Spektrální analýza (s využitím RX ASCII)*

Pak následuje krok vytvoření vlastní uSIM karty. U karet uSIM je lepší šifrování klíče a také disponují lepším bezpečnostním mechanizmem. Abychom se mohli registrovat do sítě openLTE, je nutné projít autentizačním procesem, podobně jako je tomu u GSM/UMTS/LTE. K tomu, aby bylo možné provést tento krok, je nutné znát tři parametry a to je autentizační Ki klíč, IMSI a IMEI. U parametrů IMSI a IMEI problém není to lze zjistit jednoduše, ale zjistit Ki klíč možné není, protože si ho každý operátor chrání. Tento problém, lze vyřešit programovatelnou uSIM kartou. Konkrétně u openLTE je nutné mít uSIM kartu typu sysmoUSIM-GR1 (již se nevyrábí) a sysmoUSIM-SJS1. U obou uSIM karet je nutná, podpora Milenage algoritmus, která používá autentizační metodu COMP128-4. Dalším krokem je potřeba mít zařízení, které programují SIM karty a jsou kompatibilní s PCSC aplikací Linux a podporou APDU to jsou ACR38 Smart Card Reader nebo Blutronics Bludrive II CCID. Seznam tří uSIM karet, které byly použity pro praktickou část:

- SIM Card 01:IMSI: 460110000000106
- SIM Card 02:IMSI: 460110000000107
- SIM Card 03:IMSI: 001010000000108
  Ki:00112233445566778899AABBCCDDEEFF (pro všechny tři uSIM karty)

IMEI v této diplomové práci nebude uveden, z důvodu použití osobních mobilních zařízení. Čísla budou nahrazeny písmeny x a y.

3.7 Realizace projektu openLTE

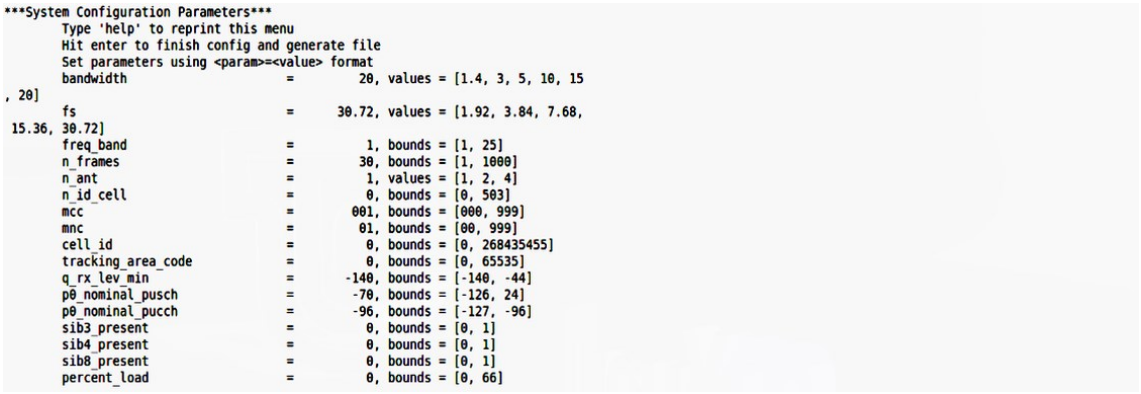
Projekt openLTE má celkem pět funkcí, které lze spustit. Můžeme si je vyzkoušet i ve Virtualboxu.

- LTE_fdd_dl_file_gen.py
- LTE_fdd_dl_file_scan.py
- LTE_fdd_dl_scan
- LTE_fdd_enodeb
- LTE_file_recorder

LTE_fdd_dl_file_gen.py slouží jen pro upřesnění, které parametry v přístupovém bodě lze nastavit a jakou hodnotu můžeme zadat. Zatímco scan.py slouží jen pro čtení základních parametrů MIB, SIB1 a SIB2. Ukázka souboru je uvedena v příloze. Klasickým editorem, nedokážeme přečíst tyto soubory, proto se musí vytvořit bin soubor, který umožní čtení z těchto souborů přes terminálové okno. Ukázka:

```
sudo touch lte_help.bin

sudo LTE_fdd_dl_file_gen/scan.py -d int8/gr_complex
lte_help.bin
```



Obrázek 3.6: *Ukázka souboru LTE_fdd_dl_file_gen.py*

V tomto souboru lze vidět, jaké hodnoty můžeme nastavit pro náš přístupový bod. Všechny parametry ale při konfiguraci nenastavíme. Není to možné provést konkrétně u fs, f_frames a percent_load. Šířku pásma (bandwidth) jak definuje LTE, lze nastavit od 1,4 do 20 MHz. Parametr fs se nastavuje při zapnutí UHD na 32,72 MHz jedná se o clock_rate. Parametr freq_band definuje pásmo, na kterém můžeme sestavit naši mobilní síť. Hodnota je od 1 do 25 a další pásma nejsou povolena. N_ant je parametr, pro počet aktivních antén. Je povoleno jen 1,2 a 4. Parametry MCC a MNC nám pomáhají při vyhledávání naší sítě pomocí mobilního zařízení. Výchozí hodnoty jsou MCC 001 a MNC 01. Cell_id můžeme nastavit libovolně. Nastavíme jen v případě, pokud chceme mít vlastní unikátní číslo základové stanice. Tracking_area_code slouží pro identifikaci naší sítě. Parametr q_rx_lev_min slouží pro minimální požadovanou úroveň RX v buňce a lze měnit od -140 dBm do -44 dBm. P0_nominal_pusch/pucch se sděluje přes SIB2 a jeden je pro směr sestupný a druhý ve směru vzestupném. SIB (Systém Information Blocks) jsou seskupeny v kontejnerech SI. Jedná se o dynamickou část, která se mapuje na RCC SI zprávách. Je jich celkem 13, ale nastavit můžeme jen 3 až 8. Parametry MIB a SIB 1 a 2 jsou pěvně zapnuty.

Dalším souborem je LTE_fdd_dl_scan, který dokáže skenovat Earfcn pro různá pásma. Samotný soubor je spustitelný, ale funkčnost není zcela v pořádku. K tomuto spuštění je potřeba zapnout v prvním terminálovém okně příkaz LTE_fdd_dl_scan a v druhém terminálovém okně se připojíme přes port 20000.

LTE_file_recorder slouží pro nahrávání parametrů. Podporované softwarově definované rádia: rtl-sdr, HackRF, BladeRF a USRP B2x0. Podobný problém jak u souboru LTE_fdd_dl_scan. K tomuto spuštění je potřeba zapnout v prvním terminálovém okně LTE_file_recorder a v druhém terminálovém okně se připojíme přes telnet na port 25000.

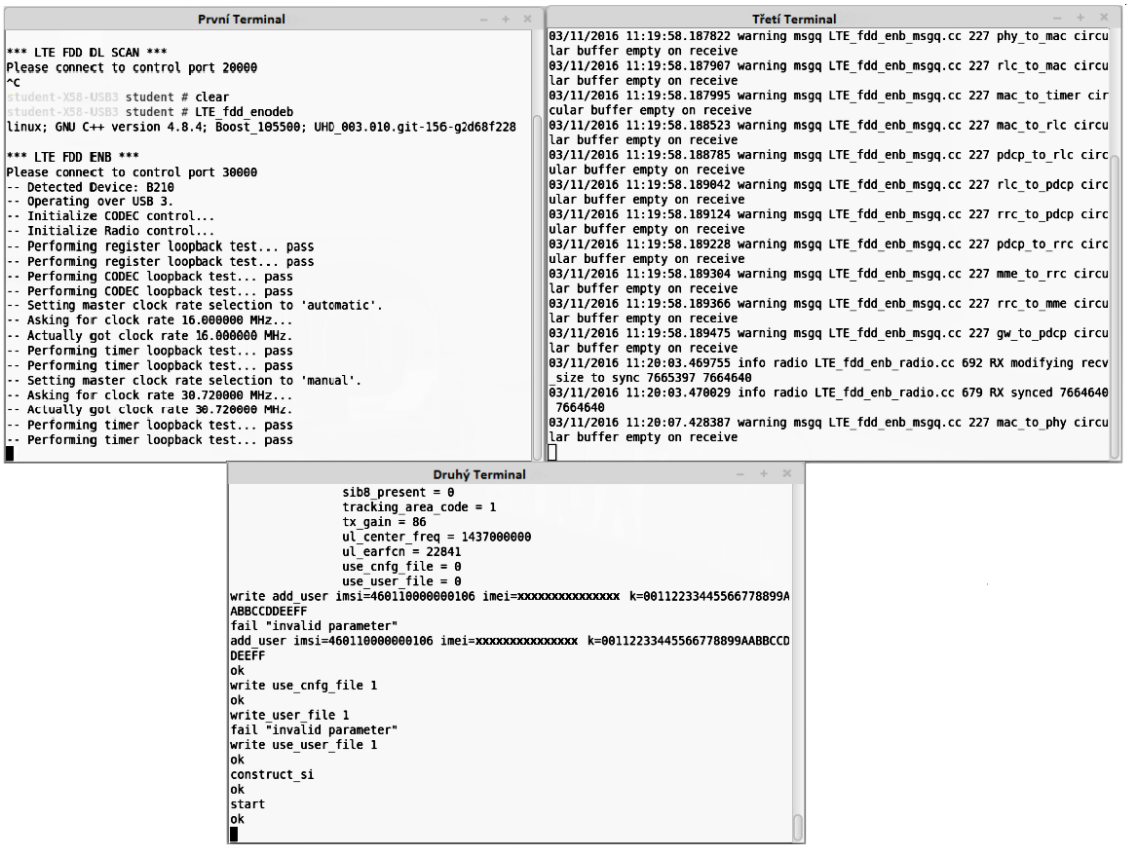
A posledním a nejdůležitějším spouštěcím souborem je LTE_fdd_enodeb. Tímto souborem budeme budovat vlastní přístupový bod (eNodeB). V současné době je podporován pouze produkt od firmy Ettus Research typu USRP B2x0. K tomu, abychom mohli zprovoznit přístupový bod, musíme použít tři terminálová okna. V prvním terminálovém okně se příkazem sudo LTE_fdd_enodeb spustí přístupový bod a bude nám zobrazovat informace o stavu desky B210. V druhém terminálovém okně se připojíme na ovládací konzoli pomocí příkazu:

```
sudo telnet 127.0.0.1/localhost 30000
```

A poslední třetí terminál přihlásíme tím samým příkazem jako u druhého terminálového okna, s tím rozdílem, že port nebude 30000 ale 30001. Zapneme okno, které nám bude vypisovat informace, chyby a signalizační procesy, které nastanou během provozu. Abychom mohli lépe analyzovat průběh celého procesu, doporučuji přesměrování výpisů z terminálového okna do souboru:

```
sudo telnet 127.0.0.1/localhost 30001
```

V případě prvního terminálového okna je lepší nesměrovat výpisy do souboru, protože při výskytu kritické chyby je nutné okamžitě ukončit proces a popřípadě znovu nahrát firmware s FPGA.



Obrázek 3.7: *Rozmístění terminálových oken na ploše*

Před samotným spuštěním je dobré se seznámit, co lze nakonfigurovat. K tomu slouží druhé terminálové okno, kde příkazem help se zobrazí, co vše lze nastavit. První příkazy start, stop a shutdown slouží pro spuštění eNodeB, zastavení eNodeB a k zastavení a ukončení eNodeB. Přidávání a mazání uživatelů z HSS slouží add_user a del_user. Pro kontrolu údajů parametrů IMSI, IMEI a Ki klíč slouží print_users. A to nejdůležitější je v System Parameters (ku pomoci slouží právě soubor LTE_fdd_dl_file_gen.py):

- band – pásmo, které podporuje LTE , souvisí s dl_earfcn (po nastavení této hodnoty se nastaví výchozí hodnota dl_earfcn).
- bandwidth - nastavitelná šířka pásma (1,7, 3, 5, 10, 15, 20). Funkční je pouze 5 MHz, u ostatních hodnot nastávají problémy s nepřipojením UE na B2X0 anebo může docházet ke kritickým chybám.
- cell_id - unikátní identifikační číslo základové stanice.
- debug_level - toto slouží pro informovanost, co přesně probíhá v průběhu spojení.
- dl_earfcn - stačí nastavit jen tento parametr s band. Protože se automaticky doplní dl_center_freq, dl_center_freq, ul_earfcn, ul_center_freq.
- dns_addr - slouží pro nastavení DNS. Tato hodnota musí být v hexadecimálním zápisu.
- enable_pcap - slouží pro ukládání záznamu, který probíhá mezi rozraní tun_openlte a UE výchozí hodnota je nastavená 0. Je potřeba ji změnit na hodnotu 1, čímž nastavíme zapnutí, a vše se ukládá do složky /tmp kde soubor je pojmenován LTE_fdd_enodeb_ip.
- ip_addr_start - jde o nastavení IP adresy na rozhraní TUN, který se vytvoří při zapnutí eNodeB. Opět je nutné IP adresu psát v hexadecimálním tvaru a nesmí kolidovat s adresou sítě.
- mcc a mnc - slouží pro identifikaci sítě, aby bylo možné ji vyhledat přes mobilní zařízení. Jedná se o kódy země a operátora.
- n_ant - počet použitých antén.
- n_id_cell - identita fyzické vrstvy buněk.
- q_hyst – hodnota hystereze obslužné buňky.
- q_rx_lev_min - minimální požadovaná úroveň RX v buňce (dBm), standardně -120 dBm.
- search_win_size - velikost okna.
- sib3 až 8 - oficiálně je jich 13, v mém případě měli všchny hodnotu 0.
- tracking_area_code - TAC identifikuje oblast sledování v rámci určité sítě.
- tx_gain - zisk vysílací antény (doporučeno 75).
- rx_gain - zisk přijímací antény (doporučeno 35). U tx_gain a rx_gain nastaveno pro laboratorní testování 5-8 dBi.
- use_cnfg_file - možnost dočasného uložení nastavené konfigurace. Nachází se v /tmp.
- use_user_file - možnost dočasného uložení všech uživatelů. Nachází se v /tmp.

Celé konfigurace parametrů z bloku System Parametres je nutné psát s write, zatím co ostatní příkazy se píši rovnou bez write. Po zapsání správné hodnoty se v terminálu objeví potvrzovací zpráva ok. Pokud bude hodnota špatně zapsaná, nebo pokud budeme dávat hodnotu mimo povolený rozsah, zobrazí se zpráva fail "invalid parameter". Před konfigurací je důležité vyhledat, jaké LTE pásma podporují mobilní zařízení. Použité mobilní zařízení pro tuto práci byly:

- LG G3 (pásmo: 3, 7, 20).
- BlackBerry Z10 (pásmo: 2, 4, 5, 17).
- Sony Xperia V (pásmo: 1, 3, 5, 7, 20).

Je důležité nalézt takové frekvenční pásmo, které podporují mobilní zařízení a zároveň se snažit nezasahovat do pásma operátora. V praktické části práce bylo použito mobilní zařízení LG G3 z důvodu nedostupnosti Sony Xperia V a BlackBerry Z10. Pásmo 20 je plně zabráno všemi operátory. Další pásma mají operátoři zakoupena, ale provoz je na nich minimální, nebo se stále testuje. Na tento fakt jsem se zaměřil a pokoušel se spektrálním analyzátorem ověřit, jestli je tomu tak. Pásma 3 a 7 byly neobsazeny a provedl jsem test pro vybudování přístupového bodu. Výsledek byl negativní, protože se nepodařilo připojit mobilní zařízení na přístupový bod. Později bylo odzkoušeno i mobilní zařízení BlackBerry Z10 opět výsledky byly negativní. Jediné pásmo, na kterém se povedla realizace, bylo pásmo 20. Pro přesné nalezení Earfcn a band byla použita webová stránka:

http://niviuk.free.fr/lte_band.php

Konfigurace, která dosahovala nejlepších výsledků, vypadá takto:

- band 20
- bandwidth 5
- cell_id 1
- debug_level radio phy mac rlc pdcp rcc mme gw user rb timer iface msgq
- debug_type error warning info debug
- dl_earfcn 6330
- dns_addr 08080808
- enable_pcap 1
- ip_addr_start C0A8016F (192.168.1.111)
- mcc 001
- mnc 01
- n_ant 2
- n_id_cell 0
- p0_nominal_pucch -96
- p0_nominal_pusch -70
- q_hyst 0
- q_rx_lev_min -120
- search_win_size 0
- sib3,4,5,6,7,8_present 0
- tracking_area_code 1
- use_user_file 1
- use_cnfg_file 1
- tx_gain 75
- rx_gain 35

Pro nastavení IP adresy a DNS, která se musí zapisovat v hexadecimálním tvaru, byla použita webová stránka:

http://ncalculators.com/digital-computation/ip-address-hex-decimal-binary.htm

Po nalezení a nakonfigurování System Parameters, je nutné přidat uživatele do HSS. K tomu slouží příkaz add_user, který přidá uživatele. Syntaxe je následující:

- add_user imsi= IMSI imei= IMEI k= Ki klíč

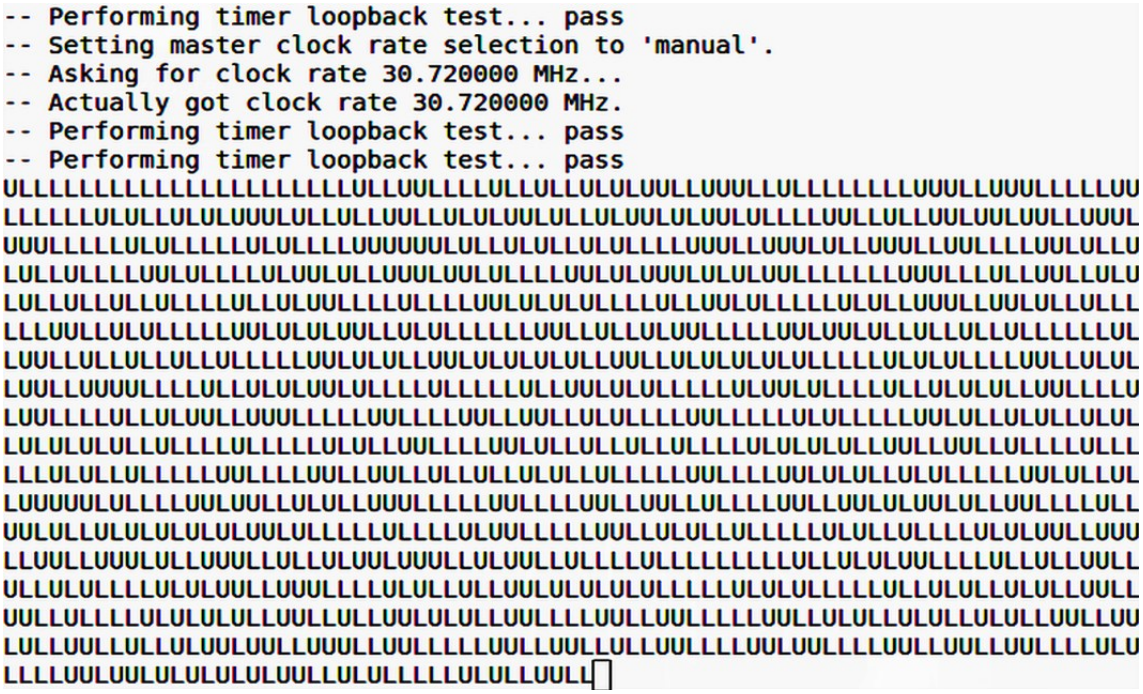
V dalším kroku je nutné nastavit APN (Access Point Name) na mobilním zařízení, aby se mohly mobilní zařízení připojit k naší nové mobilní síti. Nastavují se pouze tyto hodnoty:

- Jméno: openLTE
- APN: www.openLTE.com
- Protokol APN: IPv4
- Protokol roamingu APN: IPv4

Po nastavení všech uvedených parametrů můžeme spustit celý systém. Parametry uvedené v konfiguraci dosahovaly nejlepších výsledků. Celý systém jsem nechal běžet asi dvě až tři minuty. V prvním terminálovém okně kde běží eNodeB, indikuje zprávy typu U, L a O. Zprávy z terminálového okna viz. Obrázek 3.8:

- U - indikuje upload
- L - indikuje download
- O - indikuje, že došlo při přenosu k chybě (jedná se buď o špatnou konfiguraci, nebo o nedostatek systémových zdrojů).

Pokud se zobrazují zprávy U a L tak celý systém běží v pořádku, ale jakmile je zaznamenáno O, je lepší celý systém zastavit a zkontrolovat konfiguraci. Také může dojít během spuštění systému ke kritické chybě typu RuntimeError. IO indikuje, že selhala deska a je potřeba ji odpojit a znovu nahrát celý firmware a FPGA, protože po vypnutí eNodeB a znovu nahrání firmware a FPGA se objevila ta samá chyba. Pokud se ve zprávě vyskytuje rx(x) transfer status tak jsou špatně nastaveny parametry tx/rx gain nebo n_ant (většinou po změně se tato chyba neopakovala). A další vážný problém jsou zprávy typu recv packet demuxer unexpected SID a Got a ctrl packet with unknown. Zpráva recv packet demuxer unexpected SID indikuje, že paket byl přijat UHD, která měla neznámou SID. Tato chyba má více příčin a není na vině jen jedna věc. Zpráva Got a ctrl packet with unknown poukazuje na problém, který je zcela neznámý a jedná se problém s rozhraním mezi UHD a USB 3.0. Ve všech případech je lepší odpojit desku, počkat přibližně 10 vteřin a znovu zapojit a nahrát firmware a FPGA.



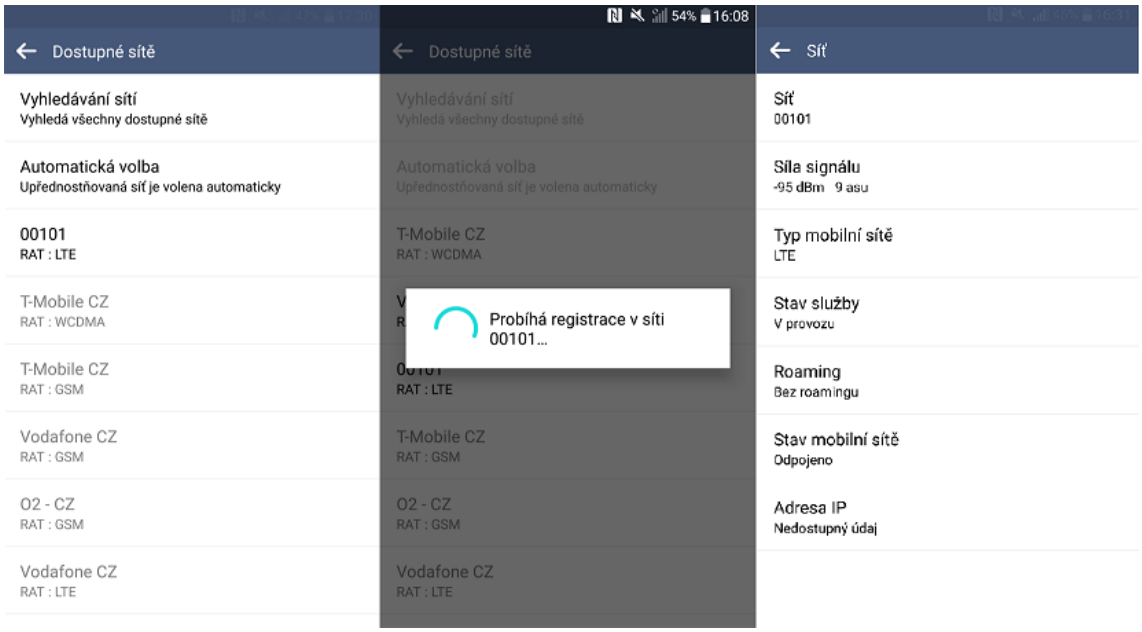
Obrázek 3.8: *Terminálové okno signalizující stav USRP B210*

V třetím terminálu, přes port 30001, lze kontroloval průběh spojení mezi UE a eNodeB. V této části byl menší problém. Pokud zůstalo zapnuté terminálové okno, celkové spojení fungovalo přibližně 30 vteřin, zatímco při vypnutém celé spojení fungovalo přes 20 minut (v jednom případě 40 minut). Jelikož jsem potřeboval ověřit a otestovat svoji konfiguraci, rozhodl jsem se vypnout terminálové okno a pracovat bez něho. Výpisy z tohoto terminálu byly přesměrovány to prázdného souboru, pro lepší analýzu. Navíc vypnutí terminálového okna umožňuje déle pracovat s celým systémem, ale nedokážeme odhalit chyby, které nastanou během přenosu.

```
on timer expiry C-RNTI=61
03/11/2016 13:14:48.069499 info user LTE_fdd_enb_user_mgr.cc 191 C-RNTI=61 relea
sed
03/11/2016 13:14:48.069565 info phy LTE_fdd_enb_phy.cc 430 Received PDSCH schedu
le from MAC CURRENT_TTI:MAC=3677,PHY=3675 N_dl_allocs=0 N_ul_allocs=1
03/11/2016 13:14:48.069619 info rb LTE_fdd_enb_rb.cc 322 SRB0 MME procedure movi
ng from IDLE to IDLE for RNTI=61
03/11/2016 13:14:48.069663 info rb LTE_fdd_enb_rb.cc 342 SRB0 MME state moving f
rom IDLE to IDLE for RNTI=61
03/11/2016 13:14:48.069676 info rb LTE_fdd_enb_rb.cc 390 SRB0 RRC procedure movi
ng from RRC CON REQ to IDLE for RNTI=61
03/11/2016 13:14:48.069685 info rb LTE_fdd_enb_rb.cc 409 SRB0 RRC state moving f
rom SRB1 SETUP to IDLE for RNTI=61
03/11/2016 13:14:48.074794 info phy LTE_fdd_enb_phy.cc 458 Received PUSCH schedu
le from MAC CURRENT_TTI:MAC=3681,PHY=3679 N_ul_decodes=1
03/11/2016 13:14:48.076586 info mac LTE_fdd_enb_mac.cc 321 UL scheduled (mcs=5,
tbs=872, N_prb=10) for RNTI=65535, UL_QUEUE_SIZE=1
03/11/2016 13:14:48.076649 info mac LTE_fdd_enb_mac.cc 1183 UL allocation sent f
or RNTI=65535 CURRENT_TTI=3691
03/11/2016 13:14:48.079568 info phy LTE_fdd_enb_phy.cc 430 Received PDSCH schedu
le from MAC CURRENT_TTI:MAC=3687,PHY=3685 N_dl_allocs=0 N_ul_allocs=1
03/11/2016 13:14:48.084583 info phy LTE_fdd_enb_phy.cc 458 Received PUSCH schedu
le from MAC CURRENT_TTI:MAC=3691,PHY=3689 N_ul_decodes=1
```

Obrázek 3.9: *Terminálové okno se signalizacemi mezi UE a eNodeB*

Mobilní zařízení vyhledala nakonfigurovanou mobilní síť a dokázala se připojit. Může se stát, že místo parametru MCC a MNC se zobrazí síť s označením Test PLMN 1-1. Při pár pokusech se stalo, že se mobilní zařízení nedokázalo připojit na mobilní síť Test PLMN 1-1. Řešení tohoto problému je jednoduché. Stačí pouze změnit parametry MCC a MNC a pak celý systém opět běží bez problémů. Dalším důležitým bodem je mít na mobilním zařízení vypnuté mobilní data z toho důvodu, že při přihlašování může celý systém selhat. Pak se musí odpojit deska od USB a napájení a nahrát znova firmware a FPGA. Mobilní data je lepší zapnout v momentě, kdy se mobilní zařízení připojí do systému a projde autentizačním procesem.



Obrázek 3.10: *Nalezení a informace o mobilní síti openLTE*

Při přihlašování do sítě se v druhém terminálovém okně, kde probíhala konfigurace eNodeB, zobrazí tři zprávy a to ověřování, uživatel plně připojen a výchozí nastavení pro uživatele.

```
imsi=001010000000108 imei=xxxxxxxxxxxxxxx   k=00112233445566778899AABBCCDDEEFF
info user authentication successful imsi=1010000000108 imei=xxxxxxxxxxxxxxx
info user fully attached imsi=1010000000108 imei=xxxxxxxxxxxxxxx
info default bearer setup for imsi=1010000000108 imei=xxxxxxxxxxxxxxx
```

Obrázek 3.11: *Přihlášení uživatele do systému*

Tento postup byl zcela v pořádku, protože po vypnutí a znovu zapnutí systému se mobilní zařízení automaticky připojovalo do mobilní sítě openLTE. Později jsem odzkoušel jiné mobilní zařízení konkrétně Sony Xperia V a bez problémů se i toto mobilní zařízení připojilo a fungovalo přibližně 20 minut.

3.8 IP provoz v openLTE

Při nalezení správné konfigurace, která je stabilní a spojení bude funkční více než 30 vteřin, se přešlo na druhou část, která je věnovaná IP provozu. V této části byl použit program Wireshark pro analýzu IP provozu. Při zapnutí přístupového bodu se zprovozní rozhraní tun_openlte, které lze ověřit příkazem ifconfig. Při této aktivaci lze programem Wiresharkem zachytávat záznamy na rozhraní tun_openlte, které probíhají mezi internetem a mobilním zařízením. V konfiguraci se musí nastavit parametr enable_pcap (LTE_fdd_enodeb_ip.pcap), který bude ukládat záznamy do složky /tmp a zkontrolovat průběh komunikace přes program Wireshark. Jak bylo uvedeno IP adresy na rozhraní tun_openlte se píší v hexadecimálním tvaru stejně tak i DNS adresa.

```
tun_openlte Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-
00-00
          inet addr:192.168.1.2  P-t-P:192.168.1.2  Mask:255.255.255.0
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

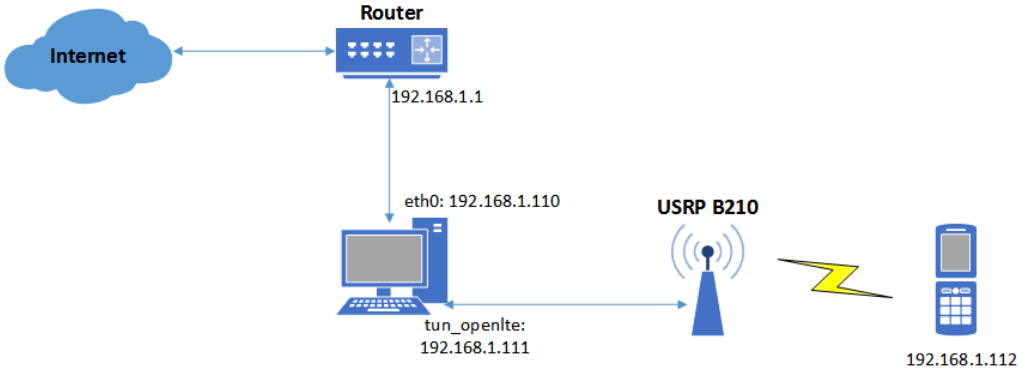
Obrázek 3.12: *Rozhraní tun_openlte*

Tento tunel umožňuje komunikaci mezi UE a vnější sítí právě přes toto TUN rozhraní. Při zapnutí mobilních a roamingových datech, mobilním zařízení okamžitě dostane IP adresu, která se nastavila automaticky při konfiguraci openLTE. Samotný tunel dostane první adresu, která se nakonfigurovala při nastavování parametru ip_addr_start. Mobilní zařízení dostane IP adresu o jednu větší. Navíc, pokud se stane, že se pravidla v iptables nenastaví automaticky při kompilaci openLTE, tak se ve složce nachází spouštěcí skript s názvem enodeb_script.sh, který při zapnutí nastaví potřebná pravidla. Než se začne pracovat, je nutné prověřit správnost pravidel v iptables a ověřit směrovací tabulku.

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.2.0.1        0.0.0.0         UG    0      0        0 eth0
10.2.0.0        0.0.0.0         255.255.254.0   U     1      0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 tun_openlte
```

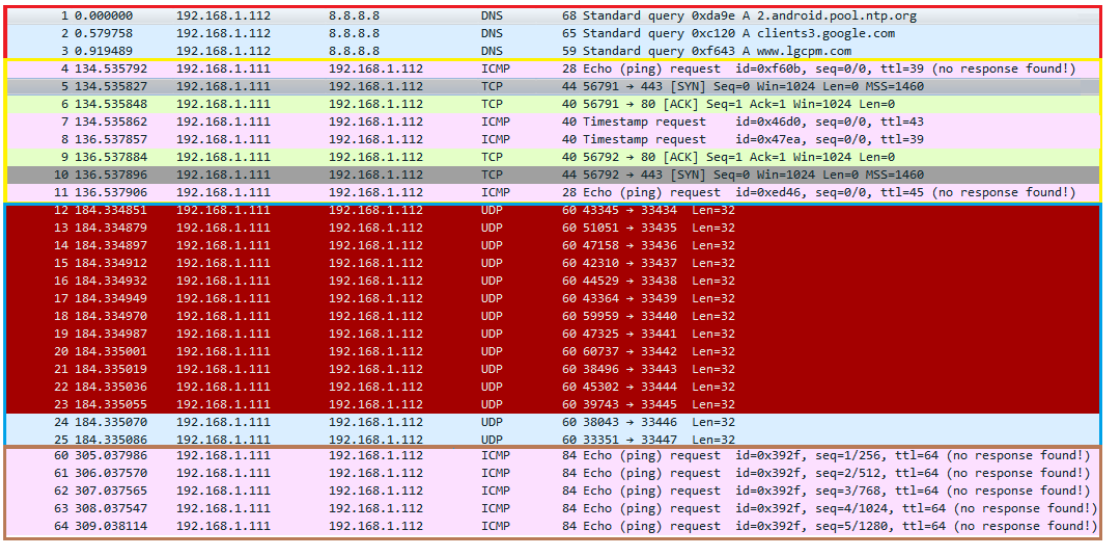
Obrázek 3.13: *Směrovací tabulka*

Po kontrole jsem přešel k ověření funkčnosti samotného IP provozu. K tomuto účelu jsem vytvořil malou síť, která byla připojena do internetu přes směrovač. Po nastavení a ověření konfigurace naše zařízení dostane odpovídající IP adresu. Pomocí programu PingTools, který je volně ke stažení do mobilních zařízení můžeme testovat ICMP z mobilního zařízení na svůj směrovač a rozhraní tun_openlte.



Obrázek 3.14: *Experimentální zapojení 1*

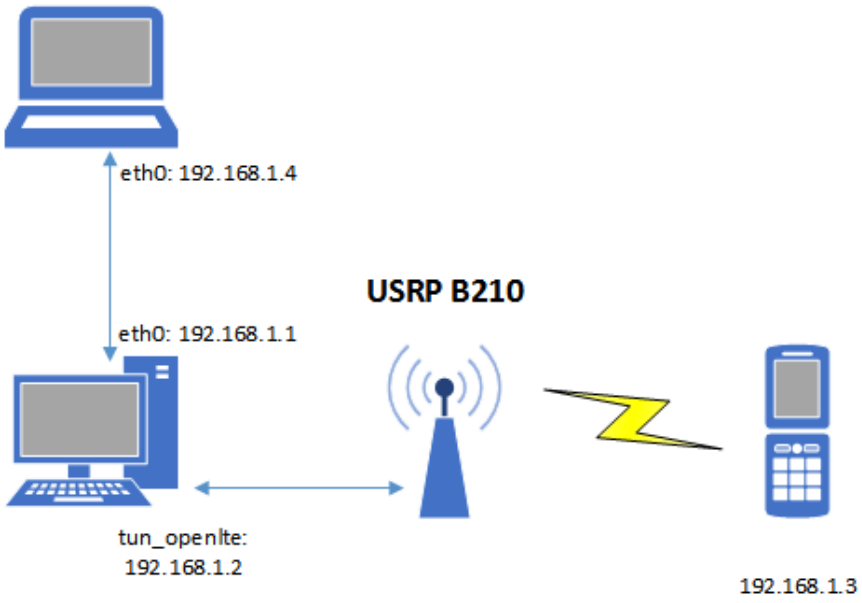
Výpisy z mobilního zařízení zobrazovaly zprávu: Vypršel časový limit žádosti (žádná odpověď). Navíc můžeme na mobilním zařízení vidět, že vzestupný směr funguje a sestupný směr nikoli.



1	0.000000	192.168.1.112	8.8.8.8	DNS	68 Standard query 0xda9e A 2.android.pool.ntp.org
2	0.579758	192.168.1.112	8.8.8.8	DNS	65 Standard query 0xc120 A clients3.google.com
3	0.919489	192.168.1.112	8.8.8.8	DNS	59 Standard query 0xf643 A www.lgcpm.com
4	134.535792	192.168.1.111	192.168.1.112	ICMP	28 Echo (ping) request id=0xf60b, seq=0/0, ttl=39 (no response found!)
5	134.535827	192.168.1.111	192.168.1.112	TCP	44 56791 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	134.535848	192.168.1.111	192.168.1.112	TCP	40 56791 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
7	134.535862	192.168.1.111	192.168.1.112	ICMP	40 Timestamp request id=0x46d0, seq=0/0, ttl=43
8	136.537857	192.168.1.111	192.168.1.112	ICMP	40 Timestamp request id=0x47ea, seq=0/0, ttl=39
9	136.537884	192.168.1.111	192.168.1.112	TCP	40 56792 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
10	136.537896	192.168.1.111	192.168.1.112	TCP	44 56792 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	136.537906	192.168.1.111	192.168.1.112	ICMP	28 Echo (ping) request id=0xed46, seq=0/0, ttl=45 (no response found!)
12	184.334851	192.168.1.111	192.168.1.112	UDP	60 43345 → 33434 Len=32
13	184.334879	192.168.1.111	192.168.1.112	UDP	60 51051 → 33435 Len=32
14	184.334897	192.168.1.111	192.168.1.112	UDP	60 47158 → 33436 Len=32
15	184.334912	192.168.1.111	192.168.1.112	UDP	60 42310 → 33437 Len=32
16	184.334932	192.168.1.111	192.168.1.112	UDP	60 44529 → 33438 Len=32
17	184.334949	192.168.1.111	192.168.1.112	UDP	60 43364 → 33439 Len=32
18	184.334970	192.168.1.111	192.168.1.112	UDP	60 59959 → 33440 Len=32
19	184.334987	192.168.1.111	192.168.1.112	UDP	60 47325 → 33441 Len=32
20	184.335001	192.168.1.111	192.168.1.112	UDP	60 60737 → 33442 Len=32
21	184.335019	192.168.1.111	192.168.1.112	UDP	60 38496 → 33443 Len=32
22	184.335036	192.168.1.111	192.168.1.112	UDP	60 45302 → 33444 Len=32
23	184.335055	192.168.1.111	192.168.1.112	UDP	60 39743 → 33445 Len=32
24	184.335070	192.168.1.111	192.168.1.112	UDP	60 38043 → 33446 Len=32
25	184.335086	192.168.1.111	192.168.1.112	UDP	60 33351 → 33447 Len=32
60	305.037986	192.168.1.111	192.168.1.112	ICMP	84 Echo (ping) request id=0x392f, seq=1/256, ttl=64 (no response found!)
61	306.037570	192.168.1.111	192.168.1.112	ICMP	84 Echo (ping) request id=0x392f, seq=2/512, ttl=64 (no response found!)
62	307.037565	192.168.1.111	192.168.1.112	ICMP	84 Echo (ping) request id=0x392f, seq=3/768, ttl=64 (no response found!)
63	308.037547	192.168.1.111	192.168.1.112	ICMP	84 Echo (ping) request id=0x392f, seq=4/1024, ttl=64 (no response found!)
64	309.038114	192.168.1.111	192.168.1.112	ICMP	84 Echo (ping) request id=0x392f, seq=5/1280, ttl=64 (no response found!)

Obrázek 3.15: *Shrnutí testů programem Wireshark rozhraní tun_openlte*

První tři záznamy z obrázku 3.15 byly z mobilního zařízení. K zobrazení došlo ihned po zapnutí mobilních a roamingových dat. Následně se spojení mezi rozhraním tun_openlte a LTE_fdd_enodeb uzavře. Po těchto třech záznamech se už z mobilního zařízení nezobrazila žádná další zpráva o navázání spojení z mobilního zařízení a naopak. Žlutě označené zprávy jsou výsledek z testu nmap, modře traceroute a hnědé řádky výpisu zobrazují ICMP zprávy z počítače na mobilní zařízení. Příkazem ARP jsem zaznamenal pouze svůj směrovač, ale neviděl jsem IP adresu svého mobilního zařízení a rozhraní tun_openlte. V této fázi nebylo jisté, jestli IP adresy jsou správně rozděleny. Provedl se tedy test správnosti rozhraní tun_openlte a využil druhého experimentálního zapojení. Celé zapojení spočívalo v přímém propojení dvou počítačů pomocí UTP kabelu. Příkazem sudo service network-manager stop zastavíme veškerý IP provoz a nastavíme IP adresy ručně. Rozhraní eth0 PC1, na kterém pracovalo openLTE, měla IP adresu 192.168.1.1/24, osobní počítač (PC2), měl IP adresu 192.168.1.4/24 a IP adresa tun_openlte měla hodnotu 192.168.1.2 (výchozí nastavení v konfiguraci).



Obrázek 3.16: *Experimentální zapojení 2*

Spustíme celý systém a programem Wireshark zapneme odchytávání na PC1 rozhraní eth0. V této části šlo pouze o ověření správnosti IP adres na rozhraní tun_opelte a mobilního zařízení. Příkazem ping, který probíhal na PC2 se testovala funkčnost rozhraní eth0 na PC1, rozhraní tun_openlte a mobilní zařízení. Připojíme mobilní zařízení na mobilní síť a zapneme mobilní a roamingové data. Ověřili jsme na mobilním zařízení, jestli byla přidělena správná IP adresa. Mobilní zařízení dostalo IP adresu 192.168.1.3. Spuštěním programu PingTool probíhal test na PC2. Výpisy z mobilního zařízení byly; opět stejné jako v předcházejícím případě. Na PC1 a PC2 byla provedena kontrola příkazem ARP a zobrazily se tyto tři záznamy. Při dalších pokusech odchytávání zpráv na rozhraní tun_openlte, nebyly zaznamenány žádné zprávy. Toto by fungovalo v případě, pokud by se podařilo dostat ICMP požadavek na mobilní zařízení a naopak.

```
Adresa HWtyp HWadresa Příznaky Maska Rozhraní
192.168.1.2              ether   1c:6f:65:3f:65:b5   C                     eth0
192.168.1.3                      (nekompletní)                           eth0
192.168.1.1              ether   1c:6f:65:3f:65:b5   C                     eth0
```

Obrázek 3.17: *Nalezení sousedů příkazem ARP*

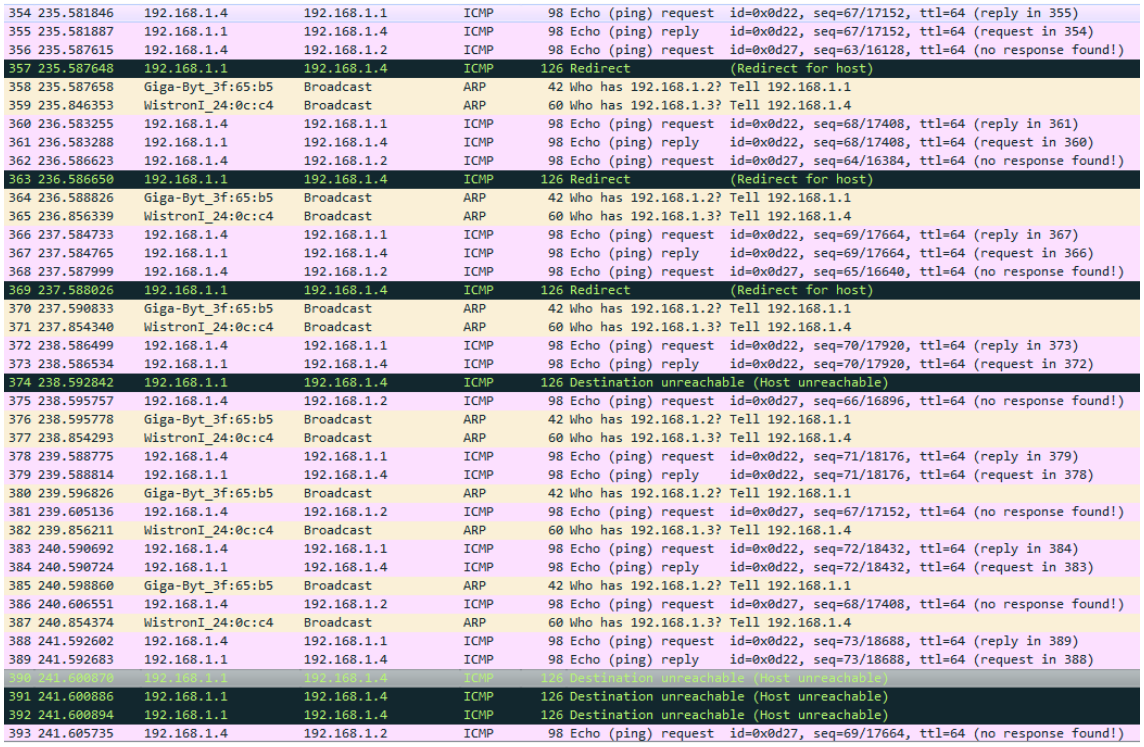
To znamenalo, že rozhraní tun_openlte pracuje správně a rozděluje správné IP adresy. Po 30 vteřinách se celý proces ukončil. Wireshark nezaznamenal žádnou zprávu o požadavku a odpovědi mezi UE a tun_openlte v souboru LTE_fdd_enodeb_ip.pcap. Kontrola souborů z PC2, kde běžel test ping, se ukazovaly následující zprávy. Ping na PC1 probíhal v pořádku celou dobu. Soubory, kde běžel test na rozhraní tun_openlte a na mobilní zařízení ukazovaly následující zprávy, viz. Obrázek 3.18. Červený záznam ukazuje průběh testu na rozhraní tun_openlte, z kterého lze vidět, jak se tunel rozpadá a následně je spojení ukončeno. V modře označeném výpisu se zobrazovala jediná zpráva typu: cílový hostitel není dostupný.

Ani při zapnutém terminálovém oknu, které zobrazovaly signalizace mezi mobilním zařízením a eNodeB, nebylo vidět, proč mobilní zařízení nedokáže dostat požadavek od počítače.

```
64 bytes from 192.168.1.2: icmp_seq=40 ttl=64 time=0.589 ms
64 bytes from 192.168.1.2: icmp_seq=41 ttl=64 time=0.527 ms
From 192.168.1.1: icmp_seq=42 Redirect Host(New nexthop: 192.168.1.2)
From 192.168.1.1: icmp_seq=43 Redirect Host(New nexthop: 192.168.1.2)
From 192.168.1.1: icmp_seq=44 Redirect Host(New nexthop: 192.168.1.2)
From 192.168.1.1: icmp_seq=45 Redirect Host(New nexthop: 192.168.1.2)
From 192.168.1.1 icmp_seq=46 Destination Host Unreachable
From 192.168.1.1 icmp_seq=47 Destination Host Unreachable
From 192.168.1.1 icmp_seq=48 Destination Host Unreachable
From 192.168.1.1 icmp_seq=49 Destination Host Unreachable
From 192.168.1.4 icmp_seq=49 Destination Host Unreachable
From 192.168.1.4 icmp_seq=50 Destination Host Unreachable
From 192.168.1.4 icmp_seq=51 Destination Host Unreachable
From 192.168.1.4 icmp_seq=52 Destination Host Unreachable
From 192.168.1.4 icmp_seq=53 Destination Host Unreachable
From 192.168.1.4 icmp_seq=54 Destination Host Unreachable
From 192.168.1.4 icmp_seq=55 Destination Host Unreachable
From 192.168.1.4 icmp_seq=56 Destination Host Unreachable
From 192.168.1.4 icmp_seq=57 Destination Host Unreachable
From 192.168.1.4 icmp_seq=58 Destination Host Unreachable
From 192.168.1.4 icmp_seq=59 Destination Host Unreachable
```

Obrázek 3.18: *Výpisy testu ping z PC2*

Po pečlivé analýze všech výpisů pingu a programu Wiresharku stále nebylo jasné, proč IP provoz není funkční, ale byla ověřena správnost rozhraní tun_openlte. Následně probíhalo dlouhé hledání na internetu a procházení diskuzního fóra projektu openLTE, kde se mi nepodařilo nalézt žádné řešení s problémem IP provozu na verzi 19.02. Jediné co se mi povedlo nalézt o IP provozu v openLTE, bylo ve verzi 18.04, který částečně fungoval. Po vyzkoušení všech řešení jsem přešel na diskuzní fórum openLTE a zaslal jsem požadavek o pomoc pro vyřešení tohoto problému. Bohužel, nebylo mi odpovězeno a nikdo na můj požadavek nereagoval. Posledním možným krokem bylo zkontaktovat studenta z minulého roku, který měl právě projekt openLTE s verzí 18.04 a zeptat se na postup při řešení mého problému. Konverzace probíhala přes webovou stránku Facebook. Po dlouhé konverzaci jsem zjistil, že postup, který jsem použil jako první experimentální zapojení 1, použil i on a nenastavoval nic speciálního, ani neměnil pravidla v iptables.



354 235.581846	192.168.1.4	192.168.1.1	ICMP	98	Echo (ping) request id=0x0d22, seq=67/17152, ttl=64 (reply in 355)
355 235.581887	192.168.1.1	192.168.1.4	ICMP	98	Echo (ping) reply id=0x0d22, seq=67/17152, ttl=64 (request in 354)
356 235.587615	192.168.1.4	192.168.1.2	ICMP	98	Echo (ping) request id=0x0d27, seq=63/16128, ttl=64 (no response found!)
357 235.587648	192.168.1.1	192.168.1.4	ICMP	126	Redirect (Redirect for host)
358 235.587658	Giga-Byt_3f:65:b5	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
359 235.846353	WistronI_24:0c:c4	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.4
360 236.583255	192.168.1.4	192.168.1.1	ICMP	98	Echo (ping) request id=0x0d22, seq=68/17408, ttl=64 (reply in 361)
361 236.583288	192.168.1.1	192.168.1.4	ICMP	98	Echo (ping) reply id=0x0d22, seq=68/17408, ttl=64 (request in 360)
362 236.586623	192.168.1.4	192.168.1.2	ICMP	98	Echo (ping) request id=0x0d27, seq=64/16384, ttl=64 (no response found!)
363 236.586650	192.168.1.1	192.168.1.4	ICMP	126	Redirect (Redirect for host)
364 236.588826	Giga-Byt_3f:65:b5	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
365 236.856339	WistronI_24:0c:c4	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.4
366 237.584733	192.168.1.4	192.168.1.1	ICMP	98	Echo (ping) request id=0x0d22, seq=69/17664, ttl=64 (reply in 367)
367 237.584765	192.168.1.1	192.168.1.4	ICMP	98	Echo (ping) reply id=0x0d22, seq=69/17664, ttl=64 (request in 366)
368 237.587999	192.168.1.4	192.168.1.2	ICMP	98	Echo (ping) request id=0x0d27, seq=65/16640, ttl=64 (no response found!)
369 237.588026	192.168.1.1	192.168.1.4	ICMP	126	Redirect (Redirect for host)
370 237.590833	Giga-Byt_3f:65:b5	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
371 237.854340	WistronI_24:0c:c4	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.4
372 238.586499	192.168.1.4	192.168.1.1	ICMP	98	Echo (ping) request id=0x0d22, seq=70/17920, ttl=64 (reply in 373)
373 238.586534	192.168.1.1	192.168.1.4	ICMP	98	Echo (ping) reply id=0x0d22, seq=70/17920, ttl=64 (request in 372)
374 238.592842	192.168.1.1	192.168.1.4	ICMP	126	Destination unreachable (Host unreachable)
375 238.595757	192.168.1.4	192.168.1.2	ICMP	98	Echo (ping) request id=0x0d27, seq=66/16896, ttl=64 (no response found!)
376 238.595778	Giga-Byt_3f:65:b5	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
377 238.854293	WistronI_24:0c:c4	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.4
378 239.588775	192.168.1.4	192.168.1.1	ICMP	98	Echo (ping) request id=0x0d22, seq=71/18176, ttl=64 (reply in 379)
379 239.588814	192.168.1.1	192.168.1.4	ICMP	98	Echo (ping) reply id=0x0d22, seq=71/18176, ttl=64 (request in 378)
380 239.596826	Giga-Byt_3f:65:b5	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
381 239.605136	192.168.1.4	192.168.1.2	ICMP	98	Echo (ping) request id=0x0d27, seq=67/17152, ttl=64 (no response found!)
382 239.856211	WistronI_24:0c:c4	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.4
383 240.590692	192.168.1.4	192.168.1.1	ICMP	98	Echo (ping) request id=0x0d22, seq=72/18432, ttl=64 (reply in 384)
384 240.590724	192.168.1.1	192.168.1.4	ICMP	98	Echo (ping) reply id=0x0d22, seq=72/18432, ttl=64 (request in 383)
385 240.598860	Giga-Byt_3f:65:b5	Broadcast	ARP	42	Who has 192.168.1.2? Tell 192.168.1.1
386 240.606551	192.168.1.4	192.168.1.2	ICMP	98	Echo (ping) request id=0x0d27, seq=68/17408, ttl=64 (no response found!)
387 240.854374	WistronI_24:0c:c4	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.4
388 241.592602	192.168.1.4	192.168.1.1	ICMP	98	Echo (ping) request id=0x0d22, seq=73/18688, ttl=64 (reply in 389)
389 241.592683	192.168.1.1	192.168.1.4	ICMP	98	Echo (ping) reply id=0x0d22, seq=73/18688, ttl=64 (request in 388)
390 241.600870	192.168.1.1	192.168.1.4	ICMP	126	Destination unreachable (Host unreachable)
391 241.600886	192.168.1.1	192.168.1.4	ICMP	126	Destination unreachable (Host unreachable)
392 241.600894	192.168.1.1	192.168.1.4	ICMP	126	Destination unreachable (Host unreachable)
393 241.605735	192.168.1.4	192.168.1.2	ICMP	98	Echo (ping) request id=0x0d27, seq=69/17664, ttl=64 (no response found!)

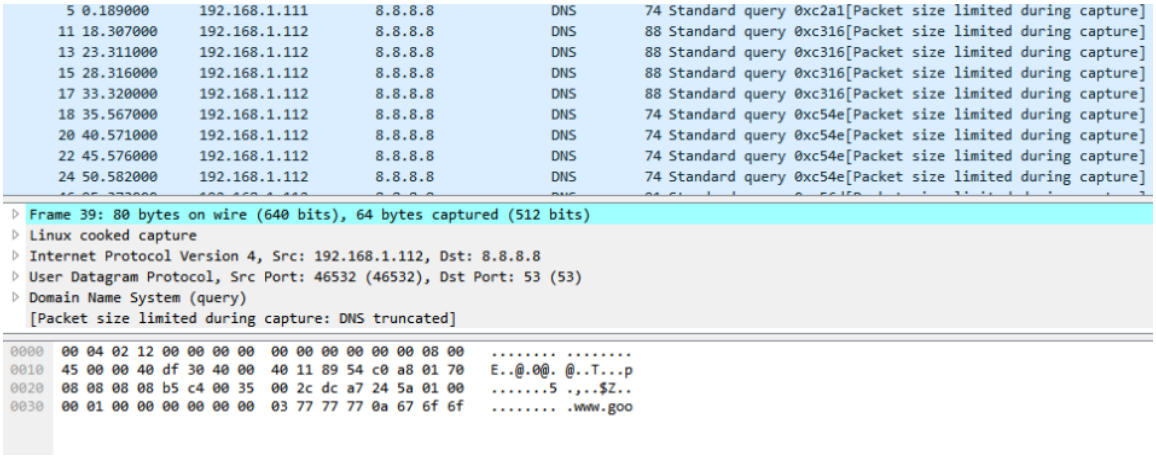
Obrázek 3.19: *Zachycení paketové komunikace programem Wireshark rozhraní eth0 na PC1*

Při hledání problémů nebylo jisté, proč zařízení nemá vlastní IP adresu, a hledal jsem nějaké řešení jak přiřadit IP adresu na desku USRP B210. Bylo divné proč rozhraní tun_openlte má inet addr stejnou IP adresu jako u P-t-P. I tento pokus selhal, protože po prozkoumání lze na USRP B210 nastavit pouze Revision, Product, Serial a Name. Jediné, kde lze přiřadit IP adresu jsou typy USRP2. Proto u tohoto typu desky musí být vytvořeno rozhraní tun_openlte, aby bylo možné přesměrovávat IP provoz z eth0 do mobilního zařízení a naopak. Tímto jsem vyčerpal veškeré možné řešení a obával jsem se, že problém není hardwarový, ale implementační. K ověření mé teorie bylo nutné vypůjčit druhé mobilní zařízení, které se připojí do mobilní sítě a otestuje se ping z prvního mobilního zařízení na druhé mobilní zařízení. Po získání mobilního zařízení, které poskytnul Bc. Kamil Ružák se provedlo experimentální zapojení 1. Rozdělení IP adres proběhlo v pořádku. Wireshark zaznamenal první tři DNS záznamy (Obrázek 3.15). Původně jsem očekával šest zpráv DNS z obou mobilních zařízení, ale zobrazili se pouze tři, to znamenalo, že při navázání spojení se uzavřela IP komunikace mezi rozhraním tun_openlte a LTE_fdd_enodeb.

```
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
*** LTE FDD ENB ***
Type help to see a list of commands
start
ok
info user authentication successful imsi=460110000000106 imei= YYYYYYYYYYYYYY
info user fully attached imsi=460110000000106 imei= YYYYYYYYYYYYYY
info default bearer setup for imsi=460110000000106 imei= YYYYYYYYYYYYYY
info user authentication successful imsi=460110000000106 imei= YYYYYYYYYYYYYY
info user authentication successful imsi=1010000000108 imei= XXXXXXXXXXXXXXX
info user fully attached imsi=1010000000108 imei= XXXXXXXXXXXXXXX
info default bearer setup for imsi=1010000000108 imei= XXXXXXXXXXXXXXX
```

Obrázek 3.20: *Připojení dvou mobilních zařízení do systému*

Program PingTool, zobrazoval zprávy typu: Vypršel časový limit žádosti (Žádná odpověď). V tuto chvíli bylo jasné, že problém je v implementaci LTE_fdd_enodeb.



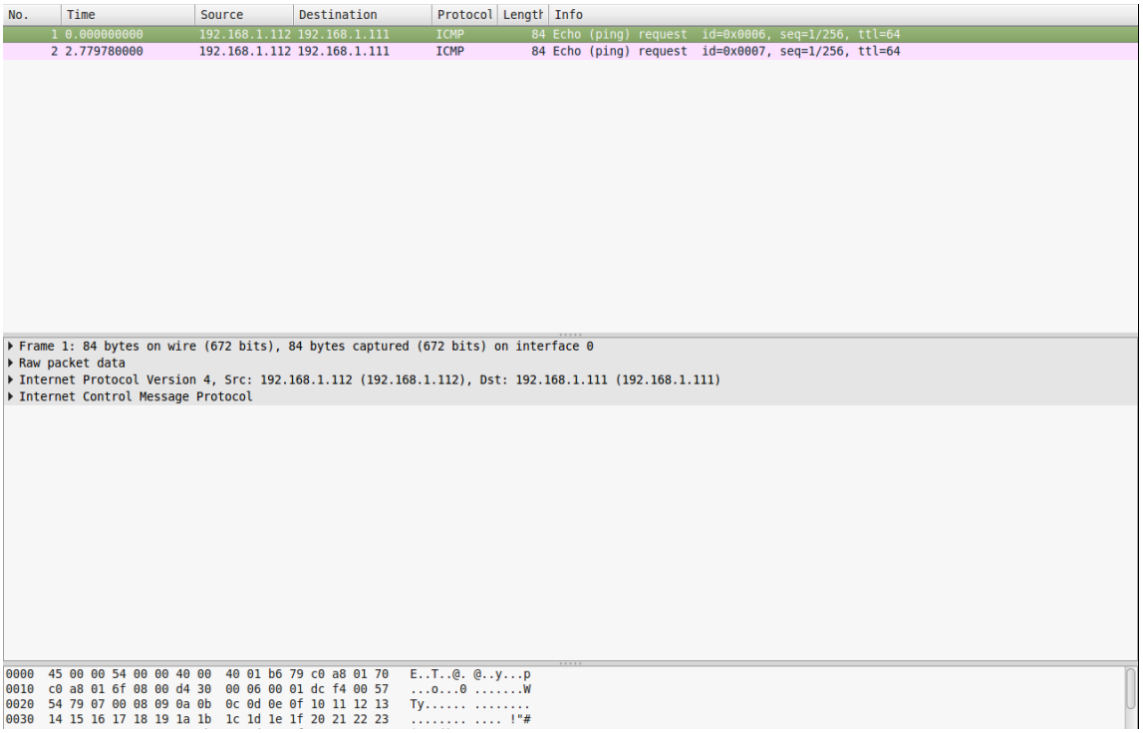
Obrázek 3.21: *Výpisy ze souboru pcap z mobilního zařízení Sony Xperia V*

Obrázek 3.21 poukazuje na problém mezi druhou a třetí vrstvou a zařízení není schopno dopravit paket do určeného cíle. Problém s fragmentací jsem vyloučil díky Obrázku 3.15, kde jsem zaznamenal tři záznamy s DNS z mobilního zařízení a vyčtením ze signalizačních zpráv ze souboru debug. IP provoz mezi UE a Internetem probíhá takto:

Internet ←→ IP stack ←→ tun_openlte ←→LTE_fdd_enodeb ←→UE

Jedinou možností bylo zkontrolovat soubory a porovnat verze 18.04 a 19.02. Zjistil jsem, že od verze 19.01 došlo k úpravám ve všech souborech a to konkrétně z boost::mutex na pthread_mutex_t a sem_t. To znamená, že při změně mohlo dojít k chybné implementaci jednoho ze souborů, který blokuje IP provoz mezi UE a rozhraním tun_openlte.

Po konzultaci s vedoucím práce bylo rozhodnuto vyzkoušet verzi 18.04 a ověřit zda je skutečně problém v implementaci. V takovém případě se musí nejprve promazat veškeré soubory, které byly naistalovány do počítače a vymazat pravidla v iptables. Po kompilaci se přešlo na ověření IP provozu. Směrovač, v den, kdy jsem testoval IP provoz, nebyl k dispozici, proto se využilo druhého experimentálního zapojení (IP adresy byli nastaveny z prvního experimentálního zapojení). Později byla provedena série pokusů podle prvního experimentálního zapojení i se směrovačem s negativními výsledky. Verze 18.04 měla obrovské problémy s udržením a navázáním spojení. Buď docházelo k selhání celého systému, nebo se mobilní zařízení nechtělo připojit na vybudovaný přístupový bod. A pokud už se síť zobrazila a mobilní zařízení se snažilo připojit, tak se v terminálu konfigurace zobrazovaly zprávy o ověření 5x a došlo k pádu. Při odchytávání rozhraní tun_openlte jsem zaznamenal požadavek z mobilního zařízení ve Wiresharku, ale nedostal žádnou odpověď, protože došlo po 5 vteřinách k chybě v prvním terminálovém okně a spojení se nestačilo navázat. Takže skutečně se jednalo o problém implementační ve verzi 19.02. Zkontroloval jsem i LTE_fdd_enodeb_ip a ukazovaly ty samé záznamy. Bohužel, výsledek uvedený pod textem byl nejlepší, který se mi povedlo zaznamenat.



Obrázek 3.22: *IP provoz verze 18.04*

4 Dosažené výsledky a zhodnocení použití openLTE

V této části diplomové práce bude popsáno, jakých výsledků bylo dosaženo v průběhu realizace projektu openLTE a celkové zhodnocení.

4.1 Porovnání verzí openLTE

V této části diplomové práce je provedeno srovnání jednotlivých verzí openLTE a zhodnocení výsledků.

4.1.1 Verze 18.04

Výše uvedená verze se v průběhu realizace jevila jako velmi nestabilní, jelikož při stejné konfiguraci jako u verze 19.02 nebylo možné spojení udržet více než 5 vteřin, nebo se mobilní zařízení vůbec nepřipojilo do sítě openLTE. Co se jevilo jako pozitivní, byla částečná funkčnost IP provozu. Příčina této nestability by mohla být i nejaktuálnějšími ovladači UHD a GNU Radia. Navíc při konfiguraci se ve verzi 18.04 parametry tx_gain a rx_gain přesunuly do Radio parameters. K dalším problémům docházelo v okamžiku pádu, nebo vypnutí systému. V těchto stavech se nastavila na obou parametrech hodnota 0. Systém nebyl schopen nalézt svou vlastní síť.

4.1.2 Verze 19.02

Verze, která byla testována jako první, měla při přihlašování a znovu napojování do mobilní sítě nejlepší výsledky. Spojení se podařilo udržet po dobu 40 minut a při dalších pokusech přibližně 20 minut. Navíc se mi povedlo připojit dvě mobilní zařízení a spojení se udrželo i se zapnutým datovým provozem přibližně 10 minut. Samozřejmě tato stabilita je funkční v okamžiku vypnutého debugového okna, které způsobovalo rozpad spojení do 30 vteřin. Protože došlo ke změně v kódu ve verzi 19.01, je vysoce pravděpodobné, že funkčnost IP provozu je blokovaná touto změnou.

4.1.3 Veze 19.03/4

V průběhu realizace mé diplomové práce vyšla verze 19.03. Podle popisu byly opraveny chyby z verze 19.02 a navíc přidána podpora HARQ. Test byl proveden ve Virtualboxu a následně byl proveden zkušební test na pevném počítači. Po kompilaci a překopírování konfiguračních souborů byl spuštěn celý proces a následně po kliknutí na Enter se všechna tři terminálová okna odpojila. Chyba byla v implementaci v n_prime_p, která byla špatně uzávorkovaná a způsobovala výše uvedené problémy. Později vyšla verze 19.04, která opravovala pouze problém s n_prime_p.

4.2 Zhodnocení a použití openLTE

V této části práce budou popsány zkušenosti a zhodnocení projektu openLTE. Konfigurování přístupového bodu je velmi jednoduché, kde přes terminálové okno můžeme jednoduše měnit nastavení parametrů. Stejně tak i kompilace projektu, kde se dá snadno kompilovat vyšší, nebo starší verze projektu. V současné době má hlavní vývojové oddělení pouze dva vývojové pracovníky, kteří se specializují na odstranění chyb a problémů v openLTE. Další členové přispívají do projektu svými poznatky, které pomáhají ve vývoji projektu openLTE.

Pro další zprovoznění přístupového bodu se dá použít pouze softwarově definované rádio od firmy Ettarus Research typ USRP B2X0. Členové zkouší i jiné softwarově definované rádia, ale zatím s negativním výsledkem. Počet členů je momentálně velmi malý pro tak rozsáhlý projekt, jako je openLTE. Pokud se podíváme na výpisy ze signalizace mezi UE a eNodeB, lze vidět, že se částečně chová jako skutečná síť LTE. Ovšem ještě dlouho potrvá, než se bude dát projekt openLTE považovat za skutečnou LTE síť. Systém openLTE se v praxi jeví jako nestabilní a to především v krocích týkajících se navázání a udržení spojení. Pásmo, které bylo zcela funkční a chovalo se stabilně, bylo pásmo 20. Při testování ostatních pásem se nedokázaly mobilní zařízení připojit. Jedinou funkční šířkou je pásmo 5 MHz. Při jiné hodnotě tohoto parametru dochází k selhání celého systému. Dosah, který dokáže udržet spojení mobilní zařízení od rádia je v rozmezí tří metrů, pak dochází k rozpadu a odpojení od vybudované mobilní sítě. Následně se pak nedokáže přístroj znovu připojit do mobilní sítě. Tento problém je částečně vyřešen ve verzi 19.04. Při hlubším testování IP provozu v openLTE, se nedokáže mobilní zařízení připojit do internetu, naopak u verze 18.04 je IP provoz částečně funkční, což dokazují výsledky uvedené v této diplomové práci. Dále pak záleží, na jakém počítači se provádí realizace eNodeB a jaké verze GNU Radio a UHD jsou používány. Celý projekt má pouze funkci připojení mobilního zařízení na přístupový bod a nemá zabudovanou podporu volání a posílání SMS. Pro další práci s openLTE doporučuji využít firmware do mobilního zařízení TEMS od firmy ASCOM, který nebyl k dispozici. Tato aplikace potlačuje Android funkce a upřednostňuje výkon antény. Touto aplikací by se dalo lépe analyzovat problémy s navázáním spojení a hlubší analýzu přenosu zpráv. Navíc dokáže ukládat výsledky do souboru pcap, takže je možné ověřovat IP provoz. Další možností je využít programu Share of Root a s touto aplikací ověřovat IP provoz.

Projekt je zaměřen pro fanoušky, které zajímá softwarově definované rádio a mobilní síť LTE. Podle informací, které jsem získal z diskuzního fóra, mají zájem i jiné univerzity, které by se chtěli zapojit a pomoci s vývojem projektu openLTE. Projekt openLTE může být použit i pro studijní účely. Po zkušenostech, které jsem získal v průběhu realizace praktické části diplomové práce, nepředpokládám, že tento projekt by měl být v blízké době využíván komerční sférou. Jedním z důvodů je nestabilita systému, nefunkční IP provoz a v neposlední řadě velmi malý dosah rádia. Dalším problém je bezpečnost provozu, který je prioritou současné doby. Tento projekt nemá bohužel zatím implementováno dostatečné zabezpečení.

Závěr

Cílem diplomové práce bylo ověřit, zda lze projekt openLTE reálně použít v praxi jako je tomu u projektů openBTS nebo openIMS. Dle dosažených výsledků se jeví, že projekt openLTE má ještě dlouhou cestu k reálnému použití v komerční sféře. Celý projekt se nachází stále ve verzi alfa a s každou verzí se upravují, nebo přidávají nové prvky, které pomáhají ve vývoji. Osobně jsem se zapojil do komunity openLTE, kde jsem se se svými připomínkami a zkušenostmi získané v průběhu realizace praktické části, podělil s ostatními členy komunity.

Významný posun jsem zaznamenal v navazování a udržení spojení mezi mobilním zařízením a přístupovým bodem. Povedlo se mi udržet spojení přibližně 20 minut v jednom případě až 40 minut. Pokud byl zapnut datový provoz, spojení fungovalo bez problémů 10 minut. K pozitivnímu výsledku přispělo i připojení dvou mobilních zařízení na vybudovaný přístupový bod.

Při testování IP provozu ve verzi 19.02, došlo kvůli implementační změně k blokaci mezi mobilním zařízením a rozraním tun_openlte.

Téma diplomové práce, kterou jsem si zvolil, mi přinesla nové zkušenosti a rozšíření znalostí problematiky USRP B210 a LTE. Velmi dobrou zkušeností bylo sledovat nové trendy, vývoj a reálné využití systému, který jsem se snažil zprovoznit. Předpokládám, že tímto má práce na projektu nekončí, ale hodlám se jí dále věnovat. Přesto že v současné době není systém vypracovaný do míry použitelné pro komerční užití, předpokládám, že je to nová forma technického řešení problému sítí a nebude trvat dlouho a najde své praktické využití.

Závěrem bych chtěl poděkovat panu doc. Ing. Miroslavu Vozňákovi Ph.D. za konzultace a snahou vyřešit problémy týkajících se projektu openLTE. Panu Ing. Janu Rozhonovi za ochotu a pomoc při nalezení chyb v mé diplomové práci a Bc. Kamilu Ružákovi za konzultace a osobní čas při řešení problémů týkající se s IP provozem a zapůjčení mobilního zařízení Sony Xperia V.

Použitá literatura

[1] Historie MTA, MTB a MTD [online] [cit. 2015-08-01] Dostupné z: http://www.radiomuseet.se/omraden/landmobil.html

[2] Historie B-Netz [online] [cit. 2015-08-10] Dostupné z: http://www.oebl.de/B-Netz/BNetz.html

[3] Technologies used 0G or Mobile Radio Telephone Systém [online] [cit. 2015-08-15] Dostupné z: http://www.cleardoubts.com/technology/technologies-used-in-0g-zero-generation-or-mobile-radio-telephone-system/

[4] Mobily za totality nesly značku Tesla. Byly jen pro vyvolené [online] [cit. 2015-08-20] Dostupné z: http://mobil.idnes.cz/mobily-za-totality-nesly-znacku-tesla-byly-jen-pro-vyvolene-pr1-/mob_tech.aspx?c=A060911_190823_mob_tech_ada

[5] Autoradiopuhelin [online] [cit. 2015-08-21] Dostupné z: http://www.myetymology.com/encyclopedia/Autoradiopuhelin.html

[6] What is 1G or First generation of wireless telecommunication technology? [online] [cit. 2015-08-22] Dostupné z: http://www.cleardoubts.com/technology/what-is-1g-or-first-generation-of-wireless-telecommunication-technology/

[7] Technologies used in 1G or First generation of Wireless Telecommunication Technology [online] [cit. 2015-08-23] Dostupné z: http://www.cleardoubts.com/technology/technologies-used-in-1g-or-first-generation-of-wireless-telecommunication-technology/

[8] Mobitex Technology [online] [cit. 2015-08-24] Dostupné z: http://www.mobitex.com/technology/default.asp

[9] Mobitex Terminal Specifications, article 1991 [online] [cit. 2015-08-24] Dostupné z: http://www.fraser-popovski.com/Mobitex.pdf

[10] MICHALEK, Libor. Rádiové sítě II, NMT. VŠB-TU Ostrava, skripta [online] 2014

[11] MICHALEK, Libor. Rádiové sítě II, ARP. VŠB-TU Ostrava, skripta [online] 2014

[12] BHALLA, Mudit Ratana a Anand Vardhan BHALLA. Generations of Mobile Wireless Technology: A Survey. International Journal of Computer Applications [online] [cit. 2015-08-22] Dostupné z: http://www.ijcaonline.org/volume5/number4/pxc3871282.pdf

[13] Generations of Wireless Communication. (From 0G to 5G). Generations of Wireless Communication. (From 0G to 5G) [online]. 2008 [cit. 2015-08-22]. Dostupné z: http://www.scribd.com/doc/124320504/Generations-of-Wireless-Communication-From-0G-to-5G#scribd

[14] MICHALEK, Libor. Rádiové sítě II, GSM. VŠB-TU Ostrava, skripta [online] 2014

[15] 3GPP - 3G GSM standards development group [online] [cit. 2015-08-22] Dostupné z: http://www.3gpp.org/

[16] What is 0.5G? [online] [cit. 2015-08-22] Dostupné z: http://www.cleardoubts.com/technology/what-is-0-5g/

[17] CSD - Circuit Switched Data [online] [cit. 2015-08-23] Dostupné z: http://www.earchiv.cz/a008s200/a008s204.php3

[18] PROKEŠ, Martin. Bezpečnostní problémy GSM. VŠB-TU Ostrava, diplomová práce [online] [cit. 2015-08-23] Dostupné z: http://hdl.handle.net/10084/103798

[19] D-AMPS (Digital-Advanced Mobile Phone Service) [online] [cit. 2015-08-23] Dostupné z: http://searchmobilecomputing.techtarget.com/definition/D-AMPS

[20] Sprint´s iDEN finally headed for sign-off [online] [cit. 2015-08-23] Dostupné z: http://www.computerworld.com/article/2514783/mobile-wireless/sprint-s-iden-finally-headed-for-sign-off.html

[21] PDC (Personal Digital Cellular) [online] [cit. 2015-08-25] Dostupné z: http://www.mobilecomms-technology.com/projects/pdc/

[22] PHS [online] [cit. 2015-08-25] Dostupné z: https://www.myjapanphone.com/Japan_cell_phone/phs.html

[23] Personal Handyphone Systém, Long Scorned, Makes Comeback [online] [cit. 2015-08-25] Dostupné z: http://www.wsj.com/articles/SB967393247519101166

[24] HSCSD (High-Speed Circuit-Switched Data) [online] [cit. 2015-08-26] Dostupné z: http://www.mobilecomms-technology.com/projects/hscsd/

[25] MICHALEK, Libor. Rádiové sítě II, Datové přenosy GSM – GPRS. VŠB-TU Ostrava, skripta [online] 2014

[26] GPRS (General Packet Radio Services) [online] [cit. 2015-08-26] Dostupné z: http://searchmobilecomputing.techtarget.com/definition/GPRS

[27] General Packet Radio Service (GPRS) [online] [cit. 2015-08-26] Dostupné z: http://www.etsi.org/technologies-clusters/technologies/mobile/gprs

[28] EDGE [online] [cit. 2015-08-26] Dostupné z: http://www.etsi.org/technologies-clusters/technologies/mobile/edge

[29] CDMA2000 1X / 1XRTT basic tutorial [online] [cit. 2015-08-27] Dostupné z: http://www.radio-electronics.com/info/cellulartelecomms/3gpp2/cdma2000-1xrtt-basics-tutorial.php

[30] The current of 2G/GSM Network [online] [cit. 2016-04-11] Dostupné z: http://www.m2mone.com.au/preparing-your-business-for-the-2g-gsm-network-shut-down-in-australia/

[31] Meaning of G, E, 2G, 3G, H, 4G in Mobile Internet Signal Bar [online] [cit 2015-08-28] Dostupné z: http://techwelkin.com/meaning-mobile-symbols-g-e-2g-3g-h-4g-mobile-internet-signal-bar

[32] What is 3G? Explained in simple terms [online] [cit. 2015-08-28] Dostupné z: http://www.3g.co.uk/PR/Feb2012/3g-what-is-3g-explained-in-simple-terms.html

[33] MICHALEK, Libor, Rádiové sítě II, UMTS, HSPA. VŠB-TU Ostrava, skripta [online] 2014

[34] VOZŇÁK, Miroslav, Spojovací systémy, IMS. VŠB-TU Ostrava, skripta [online] 2014

[35] IP IMS [online] [cit. 2015-09-03] Dostupné z: http://ipv6.com/articles/general/IP_IMS.htm

[36] IMS [online] [cit. 2015-09-03] Dostupné z: http://www.3gpp.org/technologies/keywords-acronyms/109-ims

[37] Release 4, 5, 6 [online] [cit. 2015-09-04] Dostupné z: http://www.3gpp.org/specifications/releases/

[38] IEEE 802.16 WiMAX standards [online] [cit. 2015-09-06] Dostupné z: http://www.radio-electronics.com/info/wireless/wimax/ieee-802-16-standards.php

[39] Long Term Evolution (LTE) [online] [cit. 2015-09-08] Dostupné z: http://lteworld.org/wiki/long-term-evolution-lte

[40] LTE EPS Mobility Management States [online] [cit. 2015-09-08] Dostupné z: http://www.rfwireless-world.com/Tutorials/LTE-EPS-Mobility-Management-States.html

[41] ANDSF Help Enable and “Always Best Connected“ Experience [online] [cit. 2015-09-08] Dostupné z: http://www.devicescape.com/2014/04/11/andsf-helps-enable-an-always-best-connected-experience/

[42] ANDSF MO [online] [cit. 2015-09-08] Dostupné z: http://www.3gpp.org/dynareport/24312.htm

[43] MICHALEK, Libor. Rádiové sítě II, LTE. VŠB-TU Ostrava, skripta [online] 2014

[44] LTE Network Architecture [online] [cit. 2015-09-08] Dostupné z: http://www.tutorialspoint.com/lte/lte_network_architecture.htm

[45] Protokol Signaling Procedures in LTE [online] [cit. 2015-09-08] Dostupné z: http://go.radisys.com/rs/radisys/images/paper-lte-protocol-signaling.pdf

[46] LTE-Advanced [online] [cit. 2015-11-06] Dostupné z: http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced

[47] About Ettus Research [online] [cit. 2015-11-06] Dostupné z: https://www.ettus.com/

[48] USRP B200/B210 Bus Series [online] [cit. 2015-11-06] Dostupné z: https://www.ettus.com/content/files/b200-b210_spec_sheet.pdf

[49] 3GPP TS 23.402 [online] [cit. 2015-11-08] Dostupné z: http://www.qtc.jp/3GPP/Specs/23402-a70.pdf

[50] A short history of software-defined radio (SDR) technology [online] [cit. 2015-11-09] Dostupné z: http://www.nutaq.com/blog/short-history-software-defined-radio-sdr-technology

[51] GNU Radio Companion [online] [cit. 2015-11-15] Dostupné z: http://gnuradio.org/redmine/projects/gnuradio/wiki/GNURadioCompanion

[52] PyBOMBS [online] [cit. 2015-11-15] Dostupné z: http://gnuradio.org/redmine/projects/pybombs/wiki

[53] PyBOMBS [online] [cit. 2015-11-15] Dostupné z: https://github.com/gnuradio/pybombs

[54] TOMIS, Martin, Brute Force RF modulation detection with USRP. VŠB-TU Ostrava [online]

[55] Building GNU Radio on Ubuntu Linux [online] [cit. 2016-02-24] Dostupné z: http://gnuradio.org/redmine/projects/gnuradio/wiki/UbuntuInstall

[56] Installing GNU Radio From Source [online] [cit. 2016-02-24] Dostupné z: http://gnuradio.org/redmine/projects/gnuradio/wiki/InstallingGRFromSource#Using-the-build-gnuradio-script

[57] openLTE [online] [cit. 2016-02-24] Dostupné z: http://openlte.sourceforge.net/

[58] USRP Hardware Driver Discovery Utility [online] [cit. 2016-02-17] Dostupné z: http://manpages.ubuntu.com/manpages/trusty/man1/uhd_find_devices.1.html

[59] How do I use GNU Radio? [online] [cit. 2016-02-18] Dostupné z: http://gnuradio.org/redmine/projects/gnuradio/wiki/HowToUse

[60] N. Nikaein, R. Knopp, F. Kaltenberger, L. Gauthier, Ch. Bonnet, D. Nussbaum and Riadh Ghaddab, OpenAirInterface 4G: an open LTE network in a PC. Eurecom, FRance, 2014.

Seznam příloh

Příloha A: *Ukázka souboru LTE_fdd_dl_file_scan.py*

```
***System Configuration Parameters***
        Type 'help' to reprint this menu
        Hit enter to finish config and scan file
        Set parameters using <param>=<value> format
        fs                              =      30.72, values = [1.92, 3.84, 7.68, 15.36, 30.72]

DL LTE Channel found [0]:
        MIB Decoded:
                Frequency Offset                =               0.00
                System Frame Number             =                  1
                Physical Cell ID                =                  0
                Number of TX Antennas           =                  1
                Bandwidth                       =               20MHz
                PHICH Duration                  =             Normal
                PHICH Resource                  =                  1
        SIB1 Decoded:
                PLMN Identity List:
                        001-01, Test Network, not reserved for operator use
                Tracking Area Code              =                  0
                Cell Identity                   =                  0
                Cell Barred                     =         Not Barred
                Intra Frequency Reselection     =            Allowed
                CSG Indication                  =              FALSE
                Q Rx Lev Min                    =             -140dBm
                Q Rx Lev Min Offset             =                0dB
                P Max                           =              -30dBm
                Frequency Band                  =                  1
                SI Window Length                =                2ms
                Scheduling Info List:
                        SI Periodicity = 8 frames
                        SI Window Starts at N_subframe = 0, SFN mod 8 = 0
                                SIB Type = 2
                Duplexing Mode                  =                FDD
                SI Value Tag                    =                  0
        SIB2 Decoded:
                Number of RACH Preambles        =                 64
                Power Ramping Step              =                6dB
                Preamble init target RX power   =             -100dBm
                Preamble TX Max                 =                200
                RA Response Window Size         =        10 Subframes
                MAC Contention Resolution Timer =        64 Subframes
                Max num HARQ TX for Message 3   =                  1
                Modification Period Coeff       =                  2
                Default Paging Cycle            =          256 Frames
                Modification Period             =          512 Frames
                nB                              =          256 Frames
                Root Sequence Index             =                  0
                PRACH Config Index              =                  0
                        Preamble Format = 0, RACH SFN = Even, RACH Subframe Number = 1
                High Speed Flag                 =    Unrestricted Set
                Ncs Configuration               =                  0
                PRACH Freq Offset               =                  0
                Reference Signal Power          =              -60dBm
                Pb                              =                  0
                Nsb                             =                  1
                Hopping Mode                    =      Inter Subframe
                PUSCH Nrb Hopping Offset        =                  0
                64QAM                           =            Allowed
                Group Hopping                   =           Disabled
                Group Assignment PUSCH          =                  0
                Sequence Hopping                =           Disabled
                Cyclic Shift                    =                  0
                Delta PUCCH Shift               =                  1
                N_rb_cqi                        =                  0
                N_cs_an                         =                  0
                N1 PUCCH AN                     =                  0
                P0 Nominal PUSCH                =              -70dBm
                Alpha                           =                1.0
                P0 Nominal PUCCH                =              -96dBm
                Delta F PUCCH Format 1          =                0dB
                Delta F PUCCH Format 1B         =                1dB
                Delta F PUCCH Format 2          =                0dB
                Delta F PUCCH Format 2A         =                0dB
                Delta F PUCCH Format 2B         =                0dB
                Delta Preamble Message 3        =               -2dB
                UL CP Length                    =             Normal
                T300                            =             1000ms
                T301                            =             1000ms
                T310                            =             1000ms
                N310                            =                 20
                T311                            =             1000ms
                N311                            =                 10
                Additional Spectrum Emission    =                  1
                Time Alignment Timer            =     sf500 Subframes
```